COALFIRE

WHITE PAPER

# Migration from MARS-E to ARC-AMPE System and Services Acquisition (SA) controls

## CMS requirements for Administering Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

877-224-8077 | info@coalfire.com | Coalfire.com

# Table of contents

**Purpose** ..... **2**
**Background** ..... **3**
Affordable Care Act ..... 3
CMS oversight ..... 3
ARC-AMPE ..... 3
**Control mapping** ..... **4**
System and Services Acquisition (SA) ..... 4
**References** ..... **15**
**Legal disclaimer** ..... **16**

# Purpose

This white paper provides a guide for Administering Entities (AEs) to upgrade their System Security and Privacy Plans (SSPPs) from the Minimum Acceptable Risk Standards for Exchanges (MARS-E) to the Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).

Due to the substantial number of controls, and to facilitate ease of use, this white paper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the System and Services Acquisition (SA) controls.

| ARC-AMPE Control Families | |
|---|---|
| **Control Family** | **Number of Controls** |
| Access Control | 51 |
| Awareness and Training | 9 |
| Audit and Accountability | 19 |
| Assessment, Authorization, and Monitoring | 12 |
| Configuration Management | 31 |
| Contingency Planning | 23 |
| Identification and Authentication | 24 |
| Incident Response | 16 |
| Maintenance | 16 |
| Media Protection | 9 |
| Physical and Environmental Protection | 19 |
| Planning | 6 |
| Program Management | 28 |
| Personnel Security | 9 |
| Personally Identifiable Information Processing and Transparency | 10 |
| Risk Assessment | 12 |
| **System and Services Acquisition (This Document)** | **34** |
| System and Communications Protection | 34 |
| System and Information Integrity | 34 |
| Supply Chain Risk Management | 6 |

# Background

## Affordable Care Act

The Affordable Care Act (ACA) revolutionized access to healthcare in the United States by establishing Health Insurance Marketplaces (HIMs). Enhanced Direct Enrollment (EDE) is an ACA innovation that allows third-party entities, such as insurers and web-brokers, to offer consumers a seamless application and enrollment experience directly through their platforms. This approach improves accessibility to the marketplace while maintaining compliance with federal regulations.

## CMS oversight

The Centers for Medicare & Medicaid Services (CMS) exercises oversight of AEs, which are responsible for overseeing and managing marketplace operations to ensure compliance with federal regulations, safeguard consumer data, and maintain the integrity of the HIM. Key aspects of CMS's oversight include:

- Requiring AEs to undergo rigorous audit processes, including demonstrating compliance with security and privacy control requirements.
- Enforcing strict data protection measures in the AE environment to ensure the confidentiality, integrity, and availability of consumer data and requiring entities to implement cybersecurity controls, conduct regular risk assessments, and submit independent security audits.
- Requiring AEs to adhere to operational policies and procedures, such as providing accurate plan information, maintaining transparent consumer interactions, and facilitating HIM enrollment without bias.
- Requiring AEs to report any data breaches or system incidents promptly and to take corrective actions as directed by CMS and the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).
- Requiring AEs to renew their Authority to Connect (ATC) or Authority to Operate (ATO) annually, providing updated documentation and evidence of continued compliance with all requirements.

Through these oversight mechanisms, CMS ensures that AEs in the healthcare.gov environment deliver secure, compliant, and user-friendly services, aligning with the ACA's mission to expand access to quality health coverage.

## ARC-AMPE

CMS published the ARC-AMPE Version 1.02 on April 9, 2025. This framework is slated to replace the Minimum Acceptable Risk Standards for Exchange (MARS-E) security and privacy guidelines:

- ARC-AMPE Volume 1 contains high-level guidance, and Volume 2 has the minimum-level security and privacy controls.
- ARC-AMPE Volume 2 is the new format for the SSPP for ACA AEs.
- AEs must have ARC-AMPE implemented by March 4, 2026.
- The implementation date for EDE entities has yet to be announced as of the date of this white paper.

The minimum control baseline for ARC-AMPE compliance consists of 402 controls which have been derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

The number of controls required represents a significant increase from the MARS-E baseline, and AEs should be prepared for an increased level of effort for developing the SSPP and to submit more artifacts during audits.

Another major change is the format of the SSPP template. MARS-E uses a Microsoft Word format whereas ARC-AMPE is an Excel spreadsheet.

# Control mapping

The mapping of the controls found in MARS-E Version 2.2 (based on NIST SP 800-53 Revision 4) to their new locations in ARC-AMPE (based on NIST SP 800-53 Revision 5) are included in the table below. The table lists the MARS-E control directly compared with the ARC-AMPE equivalent control name, as applicable. The table also documents any new ARC-AMPE controls that do not have MARS-E equivalents, as well as those controls that have been combined or withdrawn for ARC-AMPE.

Note also that all references to NIST SP 800-53 Revision 5 included below are based on version 5.1.1, which was issued on November 7, 2023.

## System and Services Acquisition (SA)

The set of controls in this family focus on how the Exchange shall: (1) allocate sufficient resources to adequately protect Exchange IT systems; (2) employ system development life cycle processes that incorporate IS considerations; (3) employ software usage and installation restrictions; and (4) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

| MARS-E | | ARC-AMPE | |
|---|---|---|---|
| **Control** | **System and Services Acquisition Policy and Procedures** | **Control** | **Policy and Procedures** |
| **SA-1: System and Services Acquisition Policy and Procedures**<br>The organization:<br>**a.** Develops, documents, and disseminates to applicable personnel:<br>**1.** A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>**2.** Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and<br>**b.** Reviews and updates (as necessary) the current:<br>**1.** System and services acquisition policy within every three hundred sixty-five (365) days; and<br>**2.** System and services acquisition procedures within every three hundred sixty-five (365) days. | | **SA-01: Policy and Procedures**<br>**NOTE:** *At the time of writing (March 2025) the published version of ARC-AMPE (V1.0) incorrectly lists the policy requirements for the MP family. These requirements are taken directly from NIST 800-53 Rev 5.1.1.*<br>a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:<br>1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:<br>a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and<br>2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;<br>b. Designate an [Assignment: organization-defined official] to manage the development, documentation, | |

| MARS-E | | ARC-AMPE | |
|---|---|---|---|
| | | and dissemination of the system and services acquisition policy and procedures; and<br>c. Review and update the current system and services acquisition:<br>1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and<br>2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | |
| **Control** | **Allocation of Resources** | **Control** | **Allocation of Resources** |
| **SA-2: Allocation of Resources**<br>The organization:<br>**a.** Determines information security requirements for the information system or information system service in mission/business process planning;<br>**b.** Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process;<br>**c.** Includes information security requirements in mission/business case planning;<br>**d.** Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security; and<br>**e.** Determines documents, and allocates resources required to protect the privacy and confidentiality of Personally Identifiable Information (PII) in the information system as part of the capital planning and investment control process. | | **SA-02: Allocation of Resources**<br>**a.** Determine the high-level information security and privacy requirements for the system or system service in mission and business planning;<br>**b.** Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and<br>**c.** Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation. | |
| **Control** | **System Development Life Cycle** | **Control** | **System Development Life Cycle** |
| **SA-3: System Development Life Cycle**<br>The organization:<br>**a.** Manages the information system using the formally defined and documented system development life cycle (SDLC) process that incorporates information security considerations;<br>**b.** Defines and documents information security roles and responsibilities throughout the system development life cycle;<br>**c.** Identifies individuals having information system security roles and responsibilities; and<br>**d.** Integrates the organizational information security risk management process into system development life cycle activities. | | **SA-03: System Development Life Cycle**<br>**a.** Acquire, develop, and manage the system using a formally defined and documented system development life cycle (SDLC) process that incorporates information security and privacy considerations;<br>**b.** Define and document information security and privacy roles and responsibilities throughout the SLDC;<br>**c.** Identify individuals having information security and privacy roles and responsibilities; and<br>**d.** Integrate the organizational information security and privacy risk management process into SLDC activities. | |
| **Control** | **N/A** | **Control** | **Manage Preproduction Environment** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-03(01): Manage Preproduction Environment**<br>Protect system preproduction environments commensurate with risk throughout the system development life cycle (SDLC) for the system, system component, or system service. | |
| **Control** | **N/A** | **Control** | **Use of Live Operational Data** |

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE.</td><td colspan="2">SA-03(02): Use of Live Operational Data<br>a. Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and<br>b. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.</td></tr>
<tr><th>Control</th><th>Acquisition Process</th><th>Control</th><th>Acquisition Process</th></tr>
<tr><td colspan="2">SA-4: Acquisition Process<br>The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:<br>a. Security functional requirements;<br>b. Security strength requirements;<br>c. Security assurance requirements;<br>d. Security-related documentation requirements;<br>e. Requirements for protecting security-related documentation;<br>f. Description of the information system development environment and environment in which the system is intended to operate;<br>g. Acceptance criteria; and<br>h. Requirement that providers of defined external information systems identify the location of information systems that receive, process, store, or transmit data.<br><br>Implementation Standards<br>1. Each contract and Statement of Work (SOW) that requires development or access to systems that contain PII must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR §155.260(b); define security and privacy roles and responsibilities; and receive approval from the system owner.<br>2. When contracting with external service providers:<br>a. As part of the service contract, the organization must establish security and privacy policies and procedures for how data is stored, handled, and accessed within service provider environment;<br>b. The data must be encrypted in transit to and from the service provider environment;<br>c. All mechanisms used to encrypt data must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module; and<br>d. Storage devices where data has resided must be securely sanitized according to MARS-E MP-6 Media Sanitization security control prior to use.<br>e. Per SA-9 (5), notification of the intent to outsource information system services outside the continental U.S. must be sent to CMS at least sixty (60) days prior to commitment of the outsourcing such as contract award or services purchase.</td><td colspan="2">SA-04: Acquisition Process<br>Include the following requirements, descriptions, and criteria, explicitly or by reference, using organization-defined standardized contract language in the acquisition contract for the system, system component, or system service:<br>a. Security and privacy functional requirements;<br>b. Strength of mechanism requirements;<br>c. Security and privacy assurance requirements;<br>d. Controls needed to satisfy the security and privacy requirements.<br>e. Security and privacy documentation requirements;<br>f. Requirements for protecting security and privacy documentation;<br>g. Description of the system development environment and environment in which the system is intended to operate;<br>h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and<br>i. Acceptance criteria.</td></tr>
</table>

| MARS-E | | ARC-AMPE | |
|---|---|---|---|
| **3.** When acquiring information systems, components, or services used to store, process, or transmit PII, ensure the following, in consultation with the privacy office, are included in the acquisition contract:<br>**a.** List of security and privacy controls necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements.<br>**b.** Privacy requirements set forth in the MARS-E privacy controls, including privacy training and awareness, and rules of behavior.<br>**c.** Privacy functional requirements, i.e., functional requirements specific to privacy. | | | |
| **Control** | **Functional Properties of Security Controls** | **Control** | **Functional Properties of Controls** |
| **SA-4 (1): Functional Properties of Security Controls**<br>The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. | | **SA-04(01): Functional Properties of Controls**<br>Require the developer of the system, system component, or system service to provide a description of the functional properties of the security and privacy controls to be implemented. | |
| **Control** | **Design/Implementation Information for Security Controls** | **Control** | **Design and Implementation Information for Security Controls** |
| **SA-4 (2): Design/Implementation Information for Security Controls**<br>The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed, which shall include:<br>**a.** Security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces,<br>**b.** Source code and hardware schematics; and<br>**c.** High-level design documentation at sufficient detail to prove the security control implementation. | | **SA-04(02): Design and Implementation Information for Security Controls**<br>Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes security-relevant external system interfaces, high-level design documentation, and source code or hardware schematics at organization-defined level of detail to prove the control implementation. | |
| **Control** | **Continuous Monitoring Plan** | **Control** | **N/A** |
| **SA-4 (8): Continuous Monitoring Plan**<br>The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that is commensurate with Continuous Diagnostics and Mitigation, ongoing authorization, requirements. | | **Withdrawn control**: No longer required for the minimum baseline but should still be considered best practice. | |
| **Control** | **Functions/Ports/Protocols/Services in Use** | **Control** | **Functions, Ports, Protocols, and Services in Use** |
| **SA-4 (9): Functions/Ports/Protocols/Services in Use**<br>The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the functions, ports, protocols, and services intended for organizational use. | | **SA-04(09): Functions, Ports, Protocols, and Services in Use**<br>Require the developer of the information system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use. | |
| **Control** | **Information System Documentation** | **Control** | **System Documentation** |

| MARS-E | ARC-AMPE |
|---|---|
| **SA-5: Information System Documentation**<br>The organization:<br>**a.** Obtains administrator documentation for the information system, system component, or information system service that describes:<br>**1.** Secure configuration, installation, and operation of the system, component, or service;<br>**2.** Effective use and maintenance of security functions/mechanisms; and<br>**3.** Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;<br>**b.** Obtains user documentation for the information system, system component, or information system service that describes:<br>**1.** User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;<br>**2.** Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and<br>**3.** User responsibilities in maintaining the security of the system, component, or service;<br>**c.** Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.<br>**d.** Protects documentation as required, in accordance with the risk management strategy; and<br>**e.** Distributes documentation to defined personnel or roles (defined in the applicable system security plan [SSP]).<br><br>**Implementation Standards**<br>**1.** Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.<br>**2.** Maintain an updated list of related system operations and security documentation.<br>**3.** Update documentation upon changes in system functions and processes.<br>**4.** Must include date and version number on all formal system documentation. | **SA-05: System Documentation**<br>**a.** Obtain or develop administrator documentation for the system, system component, or system service that describes:<br>**1.** Secure configuration, installation, and operation of the system, component, or service;<br>**2.** Effective use and maintenance of security and privacy functions and mechanisms; and<br>**3.** Known vulnerabilities regarding configuration and use of administrative or privileged functions;<br>**b.** Obtain or develop user documentation for the system, system component, or system service that describes:<br>**1.** User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;<br>**2.** Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and<br>**3.** User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;<br>**c.** Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take organization-defined actions in response; and<br>**d.** Distribute documentation to organization-defined personnel or roles. |
| **Control** **Security Engineering** | **Control** **Security and Privacy Engineering Principles** |
| **SA-8: Security Engineering**<br>The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. | **SA-08: Security and Privacy Engineering Principles**<br>Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: organization-defined systems security and privacy engineering principles. |
| **Control** **N/A** | **Control** **Least Privilege** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | **SA-08(14): Least Privilege**<br>Implement the security design principle of least privilege in organization-defined systems or system components. |
| **Control** **N/A** | **Control** **Trusted Communications Channels** |

| MARS-E | | ARC-AMPE | |
|---|---|---|---|
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-08(18): Trusted Communications Channels**<br>Implement the security design principle of trusted communications channels in organization-defined systems or system components. | |
| **Control** | **N/A** | **Control** | **Accountability and Traceability** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-08(22): Accountability and Traceability**<br>Implement the security design principle of accountability and traceability in organization-defined systems or system components. | |
| **Control** | **N/A** | **Control** | **Secure Defaults** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-08(23): Secure Defaults**<br>Implement the security design principle of secure defaults in organization-defined systems or system components. | |
| **Control** | **N/A** | **Control** | **Secure System Modification** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-08(31): Secure System Modification**<br>Implement the security design principle of secure system modification in organization-defined systems or system components | |
| **Control** | **N/A** | **Control** | **Sufficient Documentation** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-08(32): Sufficient Documentation**<br>Implement the security design principle of sufficient documentation in organization-defined system or system components. | |
| **Control** | **N/A** | **Control** | **Minimization** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-08(33): Minimization**<br>Implement the privacy principle of minimization using organization-defined processes. | |
| **Control** | **External Information System Services** | **Control** | **External System Services** |
| **SA-9: External Information System Services**<br>The organization:<br>**a.** Must notify CMS of plans to outsource information system services prior to the awarding of contract. Per SA-9 (5), Notification of the intent to outsource information system services outside the continental U.S. must be sent to CMS at least sixty (60) days prior to commitment of the outsourcing such as contract award or services purchase.<br>**b.** Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; | | **SA-09: External System Services**<br>**a.** Require that providers of external system services comply with organizational security and privacy requirements and employ the organization-defined controls;<br>**b.** Define and document organizational oversight and user roles and responsibilities regarding external system services; and<br>**c.** Employ defined processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: organization-defined processes, methods, and techniques. | |

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">c. Defines and documents oversight and user roles and responsibilities regarding external information system services;<br>d. Ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance; and<br>e. Employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security and privacy control compliance by external service providers on an ongoing basis.<br><br>Implementation Standards<br>1. The service contract or agreement must include language requiring the provider to be subject to U.S. Federal laws and regulations protecting PII.<br>2. The service contract or agreement must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR 155.260(b), define security and privacy roles and responsibilities.<br>3. The organization must notify CMS at least 45 days prior to transmitting data into an external information service environment.</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>Risk Assessments/Organizational Approvals</td><td>Control</td><td>Risk Assessments and Organizational Approvals</td></tr>
<tr><td colspan="2">SA-9 (1): Risk Assessments/Organizational Approvals<br>The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of information services.<br><br>Implementation Standards<br>The organization documents all existing outsourced information services and conducts a risk assessment of future outsourced information services.</td><td colspan="2">SA-09(01): Risk Assessments and Organizational Approvals<br>a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and<br>b. Verify that organization-defined personnel or roles approve the acquisition or outsourcing of dedicated information security services.</td></tr>
<tr><td>Control</td><td>Identification of Functions/Ports/Protocols/ Services</td><td>Control</td><td>Identification of Functions, Ports, Protocols, and Services</td></tr>
<tr><td colspan="2">SA-9 (2): Identification of Functions/Ports/Protocols/ Services<br>The organization requires providers of defined external information system services, as defined in the applicable system security plan, to identify the functions, ports, protocols, and other services required for the use of such services.</td><td colspan="2">SA-09(02): Identification of Functions, Ports, Protocols, and Services<br>Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: organization-defined external system services.</td></tr>
<tr><td>Control</td><td>Processing, Storage, and Service Location</td><td>Control</td><td>Processing, Storage, and Service Location</td></tr>
<tr><td colspan="2">SA-9 (5): Processing, Storage, and Service Location<br>If the organization will be maintaining PII outside of the United States, the organization must evaluate the legal environment of the country in which the information will be maintained to ensure U.S. assets are protected. The organization must coordinate with its legal counsel, privacy office, and appropriate organization representative in meeting this requirement.</td><td colspan="2">SA-09(05): Processing, Storage, and Service Location<br>Restrict the location of information processing, information or data, and system services to organization-defined locations based on organization-defined requirements or conditions.</td></tr>
</table>

| MARS-E | | ARC-AMPE | |
|---|---|---|---|
| The organization restricts the location of information processing, information/data, and information system services to organization-defined locations based on program requirements or conditions. In no case may the safeguards afforded to sensitive information be less than the safeguards mandates by state regulation, federal law, Executive Order, or other authoritative direction.<br>Notification of the intent to outsource information system services outside the continental U.S. must be sent to CMS at least sixty (60) days prior to commitment of the outsourcing such as contract award or services purchase. Depending on the outcome of the risk assessment, the organization may need to restrict the location of information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations. | | | |
| **Control** | **N/A** | **Control** | **Processing and Storage Location – U.S. Jurisdiction** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-09(08): Processing and Storage Location – U.S. Jurisdiction**<br>Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States. | |
| **Control** | **Developer Configuration Management** | **Control** | **Developer Configuration Management** |
| **SA-10: Developer Configuration Management**<br>The organization requires the developer of the information system, system component, or information system service to:<br>**a.** Perform configuration management during system, component, or service development, implementation, and operation;<br>**b.** Document, manage, and control the integrity of changes to organization-defined configuration items under configuration management;<br>**c.** Implement only organization-approved changes to the system, component, or service;<br>**d.** Document approved changes to the system, component, or service and the potential security impacts of such changes; and<br>**e.** Track security flaws and flaw resolution within the system, component, or service and report findings to defined organization-defined personnel or roles (defined in the applicable system security plan). | | **SA-10: Developer Configuration Management**<br>Require the developer of the system, system component, or system service to:<br>**a.** Perform configuration management during system, component, or service design, development, implementation, operation, and disposal;<br>**b.** Document, manage, and control the integrity of changes to organization-defined configuration items under configuration management.<br>**c.** Implement only organization-approved changes to the system, component, or service;<br>**d.** Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and<br>**e.** Track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles. | |
| **Control** | **Software/Firmware Integrity** | **Control** | **Software and Firmware Integrity Verification** |
| **SA-10 (1): Software/Firmware Integrity**<br>The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components. | | **SA-10(01): Software and Firmware Integrity Verification**<br>Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components. | |

| MARS-E | | ARC-AMPE | |
|---|---|---|---|
| **Control** | **Developer Security Testing and Evaluation** | **Control** | **Developer Testing and Evaluation** |
| **SA-11: Developer Security Testing and Evaluation**<br>The organization requires the developer of the information system, system component, or information system service to:<br>**a.** Create and implement a security assessment plan in accordance with, but not limited to, current organization procedures;<br>**b.** Perform unit; integration; system; regression testing/evaluation in accordance with organizational defined system development life cycle;<br>**c.** Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;<br>**d.** Implement a verifiable flaw remediation process; and<br>**e.** Correct flaws identified during security testing/evaluation.<br>**f.** Conduct tests that:<br>**1.** Minimize to the use of PII to the maximum extent practicable;<br>**2.** Use actual PII only if a formal memorandum of agreement (MOA), memorandum of understanding (MOU), or data exchange agreement has been established between the data owner of the PII and the entity developing/testing the information system, including how to handle loss, theft, or compromise (i.e., breach) of PII;<br>**3.** Use de-identified or anonymized PII to the maximum extent practicable; and<br>**4.** Coordinate use of PII with the organization's privacy office before conducting any testing.<br><br>**Implementation Standards**<br>**1.** If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made after the assessment and after selective verification of the results.<br>**2.** Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.<br>**3.** All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing and is restricted by source and destination access control lists as well as ports and protocols. | | **SA-11: Developer Testing and Evaluation**<br>Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:<br>**a.** Develop and implement a plan for ongoing security and privacy control assessments;<br>**b.** Perform unit, integration, system, and regression testing/evaluation in accordance with the organizational-defined frequency at organization-defined depth and coverage;<br>**c.** Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;<br>**d.** Implement a verifiable flaw remediation process; and<br>**e.** Correct flaws identified during testing and evaluation. | |
| **Control** | **Static Code Analysis** | **Control** | **Static Code Analysis** |
| **SA-11 (1): Static Code Analysis**<br>The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis. | | **SA-11(01): Static Code Analysis**<br>Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis. | |
| **Control** | **Threat and Vulnerability Analysis** | **Control** | **Threat Modeling and Vulnerability Analysis** |

| MARS-E | | ARC-AMPE | |
|---|---|---|---|
| **SA-11 (2): Threat and Vulnerability Analysis**<br>The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service. | | **SA-11(02): Threat Modeling and Vulnerability Analysis**<br>Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and subsequent testing and evaluation of the system, component, or service that:<br>**a.** Uses the following contextual information: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels;<br>**b.** Employs organization-defined tools and methods;<br>**c.** Conducts the modeling and analyses at the following level of rigor: organization-defined breadth and depth of modeling and analyses; and<br>**d.** Produces evidence that meets organization-defined acceptance criteria. | |
| **Control** | **Dynamic Code Analysis** | **Control** | **Dynamic Code Analysis** |
| **SA-11 (8): Dynamic Code Analysis**<br>The organization requires information systems, system components, and information system services to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. | | **SA-11(08): Dynamic Code Analysis**<br>Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. | |
| **Control** | **N/A** | **Control** | **Development Process, Standards, and Tools** |
| Existing NIST SP 800-53 Rev. 4 control and new to ARC-AMPE. | | **SA-15: Development Process, Standards, and Tools**<br>**a.** Require the developer of the system, system component, or system service to follow a documented development process that:<br>**1.** Explicitly addresses security and privacy requirements;<br>**2.** Identifies the standards and tools used in the development process;<br>**3.** Documents the specific tool options and tool configurations used in the development process; and<br>**4.** Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and<br>**b.** Review the development process, standards, tools, tool options, and tool configurations at least every one (1) year or as needed to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization-defined security and privacy requirements. | |
| **Control** | **N/A** | **Control** | **Minimize Personally Identifiable Information** |
| New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE. | | **SA-15(12): Minimize Personally Identifiable Information**<br>Require the developer of the system or system component to minimize the use of Personally Identifiable Information (PII) in development and test environments. | |
| **Control** | **N/A** | **Control** | **Developer Security Architecture and Design** |
| Existing NIST SP 800-53 Rev. 4 control and new to ARC-AMPE. | | **SA-17: Developer Security Architecture and Design** | |

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2"></td><td colspan="2">Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:<br>a. Is consistent with the organization’s security and privacy architecture that is an integral part the organization’s enterprise architecture;<br>b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and<br>c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Developer Screening</td></tr>
<tr><td colspan="2">Existing NIST SP 800-53 Rev. 4 control and new to ARC-AMPE.</td><td colspan="2">SA-21: Developer Screening<br>Require that the developer of systems, system components, or system services:<br>a. Has appropriate access authorizations as determined by the assigned Authorizing Official (AO) or Designee; and;<br>b. Satisfies personnel screening criteria consistent with PS-3.</td></tr>
<tr><td>Control</td><td>Unsupported System Components</td><td>Control</td><td>Unsupported System Components</td></tr>
<tr><td colspan="2">SA-22: Unsupported System Components<br>The organization:<br>a. Replaces information system components as soon as possible after discovery that support for the components is no longer available from the developer, vendor, or manufacturer; and<br>b. Where immediate replacement is not possible, provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.</td><td colspan="2">SA-22: Unsupported System Components<br>a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or<br>b. Provide the following option(s) for alternative sources for continued support for unsupported components: provide justification and document the approval for the continued use of unsupported system components required to satisfy mission/business needs.</td></tr>
</table>

# References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

CMS Standards

# Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

## About the authors

**Jessica Payne**, Consultant

Jessica joined Coalfire in 2024 with five prior years of cybersecurity consulting experience. She supports our clients as a Consultant for the GRC Healthcare team where she specializes in cybersecurity risk management, cybersecurity program advisory, and compliance for the healthcare industry.

Her extensive experience in cybersecurity consulting allows her to provide customized solutions and guidance on industry best practices, greatly improving client security postures and ensuring compliance with regulatory standards. She is dedicated to ongoing improvement and to staying abreast of the latest cybersecurity trends and technologies to offer innovative solutions to her clients.

**Ian Walters,** Principal

Ian is a seasoned cybersecurity professional with a wealth of experience across a spectrum of frameworks and standards, including NIST SP 800-53, HIPAA, ISO 27001, ISO 20000, and ISO 9001.

With a meticulous eye for detail and a strategic mindset, Ian excels in developing tailored solutions to ensure compliance and mitigate risks within complex organizational environments. His expertise extends to leading audits and risk assessments, as well as providing advisory for driving continuous improvement initiatives to enhance cybersecurity posture and operational resilience.

## About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

Copyright © 2025 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_ACA CMS Controls Migration (System and Services Acquisition (SA)) 03262025