COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE System and Communications Protection (SC) controls

CMS requirements for Administering Entities

IAN WALTERS, PRINCIPAL
JESSICA PAYNE, CONSULTANT

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 Communications Protection (SC) 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 Communications Protection (SC) 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	34
System and Communications Protection (This Document)	**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 Communications Protection (SC)

The set of controls in this family focus on how the Exchange shall: (1) monitor, control, and protect Exchange communications (i.e., information transmitted or received by Exchange IT systems) at the external boundaries and key internal boundaries of the IT systems; and (2) employ architectural designs, software development techniques, and systems engineering principles that promote effective IS within Exchange IT systems.

MARS-E		ARC-AMPE	
Control	**System and Communications Protection Policy and Procedures**	**Control**	**Policy and Procedures**
SC-1: System and Communications Protection Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and **b.** Reviews and updates (as necessary) the current: **1.** System and communications protection policy within every three hundred sixty-five (365) days; and **2.** System and communications protection procedures within every three hundred sixty-five (365) days.		**SC-01: Policy and Procedures** **a.** Develop, document, and disseminate to organization-defined personnel and roles: **1.** Organization-level system and communications protection policy that: **(a)** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **(b)** Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and **2.** Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; **b.** Designate an organization-defined official to manage the deployment, documentation, and dissemination of the system and communications protection policy and procedures; and **c.** Review and update (as necessary) the current system and communications protection: **1.** Policy at least every one (1) year and following organization-defined events; and **2.** Procedures at least every (1) year and following organization-defined events.	

MARS-E		ARC-AMPE	
Control	**Application Partitioning**	**Control**	**Separation of System and User Functionality**
SC-2: Application Partitioning The information system separates user functionality, including user interface services (e.g., web services), from information system management (e.g., database management systems) functionality. In any situation where personally identifiable information (PII) is present, PII must be stored on a logical or physical partition separate from the applications and software partition.		**SC-02: Separation of System and User Functionality** Separate user functionality, including user interface services, from system management functionality.	
Control	**N/A**	**Control**	**Interfaces for Non-Privileged Users**
Existing NIST SP 800-53 Rev.4 control which was not selected for MARS-E 2.2 and is applicable to ARC-AMPE.		**SC-02(01): Interfaces for Non-Privileged Users** Prevent the presentation of system management functionality at interfaces to non-privileged users.	
Control	**Information in Shared Resources**	**Control**	**Information in Shared System Resources**
SC-4: Information in Shared Resources The information system prevents unauthorized and unintended information transfer via shared system resources. **Implementation Standards** **1.** Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. **2.** Ensure that system resources shared between two (2) or more users are released back to the information system and are protected from accidental or purposeful disclosure.		**SC-04: Information in Shared System Resources** Prevent unauthorized and unintended information transfer via shared system resources.	
Control	**Denial of Service Protection**	**Control**	**Denial-of-Service Protection**
SC-5: Denial of Service Protection The information system protects against or limits the effects of the types of denial-of-service attacks defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable security plan): **a.** SANS Organization: www.sans.org/dosstep; **b.** SANS Organization's Roadmap to Defeating Denial of Service (DDoS): www.sans.org/dosstep; and **c.** NIST National Vulnerability Database: http://nvd.nist.gov/cvss.cfm. **Implementation Standards** The organization defines a list of types of denial-of-service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list.		**SC-05: Denial-of-Service Protection** **a.** Protect against the effects of the following denial-of-service event types: at a minimum, Internet Control Message Protocol (ICMP) flood, SYN flood, slowloris, buffer overflow attack, and volume attack; and **b.** Employ the following controls to achieve the denial-of-service objective: organization-defined controls by type of denial-of-service event.	
Control	**N/A**	**Control**	**Restrict Ability to Attack Other Systems**

MARS-E		ARC-AMPE	
Existing NIST SP 800-53 Rev.4 control which was not selected for MARS-E 2.2 and is applicable to ARC-AMPE.		**SC-05(01): Restrict Ability to Attack Other Systems** Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: organization-defined denial-of-service attacks.	
Control	**N/A**	**Control**	**Capacity, Bandwidth, and Redundancy**
Existing NIST SP 800-53 Rev.4 control which was not selected for MARS-E 2.2 and is applicable to ARC-AMPE.		**SC-05(02): Capacity, Bandwidth, and Redundancy** Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	
Control	**N/A**	**Control**	**Detection and Monitoring**
Existing NIST SP 800-53 Rev.4 control which was not selected for MARS-E 2.2 and is applicable to ARC-AMPE.		**SC-05(03): Detection and Monitoring** **a.** Employ organization-defined monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system; and **b.** Monitor organization-defined system resources to determine if sufficient resources exist to prevent effective denial of service attacks.	
Control	**Resource Availability**	**Control**	**N/A**
SC-6: Resource Availability **FOR CLOUD ENVIRONMENT ONLY** The information system protects the availability of resources by allocating resources by priority and/or quota.		Withdrawn from the minimum baseline.	
Control	**Boundary Protection**	**Control**	**Boundary Protection**
SC-7: Boundary Protection The information system: **a.** Monitors and controls communications at the external boundary, both physically and logically, of the system and at key internal boundaries within the system; **b.** Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and **c.** Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. **Implementation Standards** **1.** Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. **2.** Utilize stateful inspection/application firewall hardware and software. **3.** Utilize firewalls from at least two (2) or more different vendors at the various levels within the network to reduce the possibility of compromising the entire network. **4.** If the system has an outward facing Web or email presence to the public internet, the organization must implement and support a technical capability to detect malware in web traffic traversing the organization's boundary by:		**SC-07: Boundary Protection** **a.** Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; **b.** Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and **c.** Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	

MARS-E		ARC-AMPE	
a. Monitoring assets without the need to deploy software agents (zero client footprint); **b.** Dynamically generating actionable malware intelligence; **c.** Detecting and stopping web-based and email attacks; and **d.** Sending alert data to the organization's security information event management (SIEM) system.			
Control	**Access Points**	**Control**	**Access Points**
SC-7 (3): Access Points The organization limits the number of external network connections to the information system.		**SC-07(03): Access Points** Limit the number of external network connections to the system.	
Control	**External Telecommunications Services**	**Control**	**External Telecommunications Services**
SC-7 (4): External Telecommunications Services The organization: **a.** Implements a managed interface for each external telecommunication service; **b.** Establishes a traffic flow policy for each managed interface; **c.** Protects the confidentiality and integrity of the information transmitted across each interface; **d.** Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and **e.** Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of a major new system, and removes exceptions that are no longer supported by an explicit mission/business need.		**SC-07(04): External Telecommunications Services** **a.** Implement a managed interface for each external telecommunication service; **b.** Establish a traffic flow policy for each managed interface; **c.** Protect the confidentiality and integrity of the information being transmitted across each interface; **d.** Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need; **e.** Review exceptions to the traffic flow policy within every one (1) year or whenever there is a change in the threat environment that warrants a review of the exceptions and remove exceptions that are no longer supported by an explicit mission or business need; **f.** Prevent unauthorized exchange of control plane traffic with external networks; **g.** Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and **h.** Filter unauthorized control plane traffic from external networks.	
Control	**Deny by Default/Allow by Exception**	**Control**	**Deny By Default — Allow By Exception**
SC-7 (5): Deny by Default/Allow by Exception The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).		**SC-07(05): Deny By Default — Allow By Exception** Deny network communications traffic by default and allow network communications traffic by exception: at managed interfaces as documented in the applicable System Security and Privacy Plan (SSPP).	
Control	**Prevent Split Tunneling for Remove Drivers**	**Control**	**Split Tunneling for Remote Devices**
SC-7 (7): Prevent Split Tunneling for Remove Drivers The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.		**SC-07(07): Split Tunneling for Remote Devices** Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using organization-defined security safeguards.	
Control	**Route Traffic to Authenticated Proxy Servers**	**Control**	**Route Traffic to Authenticated Proxy Servers**
SC-7 (8): Route Traffic to Authenticated Proxy Servers		**SC-07(08): Route Traffic to Authenticated Proxy Servers**	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.

Implementation Standards
The organization defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by the organizational Authorizing Authority.</td><td colspan="2">Route organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.</td></tr>
<tr><td>Control</td><td>Host-Based Protection</td><td>Control</td><td>Host-Based Protection</td></tr>
<tr><td colspan="2">SC-7 (12): Host-Based Protection
The organization implements defined, host-based boundary protection mechanisms at defined information system components, including servers, workstations, and mobile devices.</td><td colspan="2">SC-07(12): Host-Based Protection
Implement Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or at a minimum a host-based firewall at organization-defined system components.</td></tr>
<tr><td>Control</td><td>Isolation of Security Tools</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">SC-7 (13): Isolation of Security Tools
The organization defines key information security tools, mechanisms, and support components associated with system and security administration; and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets</td><td colspan="2">Withdrawn from the minimum baseline.</td></tr>
<tr><td>Control</td><td>Fail Secure</td><td>Control</td><td>Fail Secure</td></tr>
<tr><td colspan="2">SC-7 (18): Fail Secure
The information system fails securely in the event of an operational failure of a boundary protection device.</td><td colspan="2">SC-07(18): Fail Secure
Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Boundary Protection | Personally Identifiable Information</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE.</td><td colspan="2">SC-07(24): Boundary Protection | Personally Identifiable Information
For systems that process Personally Identifiable Information (PII):
a. Apply the following processing rules to data elements of PII: processing rules for compliance with ACA, Privacy Act, and other applicable PII processing laws and regulations.
b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
c. Document each processing exception; and
d. Review and remove exceptions that are no longer supported.</td></tr>
</table>

MARS-E		ARC-AMPE	
Control	**N/A**	**Control**	**Boundary Protection | Separate Subnets to Isolate Functions**
New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE.		**SC-07(29): Boundary Protection | Separate Subnets to Isolate Functions** Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.	
Control	**Transmission Confidentiality and Integrity**	**Control**	**Transmission Confidentiality and Integrity**
SC-8: Transmission Confidentiality and Integrity The information system protects the confidentiality and integrity of transmitted information. Any transmitted data containing sensitive information must be encrypted using a FIPS 140-2 validated module (see SC-13).		**SC-08: Transmission Confidentiality and Integrity** Protect the confidentiality and integrity of transmitted information.	
Control	**Cryptographic or Alternate Physical Protection**	**Control**	**Cryptographic Protection**
SC-8 (1): Cryptographic or Alternate Physical Protection The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by approved alternative safeguards and defined in the applicable system security plan and Information Risk Assessment. FIPS-validated encryption or protected distribution systems are used to protect PII to ensure the information's confidentiality and integrity during transmission. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(6).		**SC-08(01): Cryptographic Protection** Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.	
Control	**Pre/Post Transmission Handling**	**Control**	**Pre- and Post-Transmission Handling**
SC-8 (2): Pre/Post Transmission Handling The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.		**SC-08(02): Pre- and Post-Transmission Handling** Maintain the confidentiality and integrity of information during preparation for transmission and during reception.	
Control	**Network Disconnect**	**Control**	**Network Disconnect**
SC-10: Network Disconnect The information system: **a.** Terminates the network connection associated with a communications session at the end of the session, or: **1.** Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and **2.** Forcibly disconnects inactive VPN connections after thirty (30) minutes or less of inactivity; and **b.** Terminates or suspends network connections (i.e., a system-to-system interconnection) upon issuance of an order by the organization's Chief Information Officer (CIO), Chief Information Security Officer (CISO), or Senior Official for Privacy (SOP).		**SC-10: Network Disconnect** Terminate the network connection associated with a communications session at the end of the session or after thirty (30) minutes for privileged sessions and no longer than sixty (60) minutes for general user sessions of inactivity.	

MARS-E		ARC-AMPE	
Implementation Standards **1.** The information system terminates the network connection associated with a communications session at the end of the session, or after thirty (30) minutes for all RAS-based sessions and thirty (30) to sixty (60) minutes for non-interactive users, of inactivity. **2.** Long running batch jobs and other operations are not subject to this time limit.			
Control	**Cryptographic Key Establishment and Management**	**Control**	**Cryptographic Key Establishment and Management**
SC-12: Cryptographic Key Establishment and Management When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with defined organizational requirements (defined in, or referenced by, the applicable security plan) for key generation, distribution, storage, access, and destruction.		**SC-12: Cryptographic Key Establishment and Management** Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: organization-defined requirements for key generation, distribution, storage, access, and destruction.	
Control	**Symmetric Keys**	**Control**	**N/A**
SC-12 (2): Symmetric Keys The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes.		Withdrawn from the minimum baseline.	
Control	**Asymmetric Keys**	**Control**	**N/A**
SC-12 (3): Asymmetric Keys The organization produces, controls, and distributes asymmetric cryptographic keys using NIST FIPS-compliant key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; and approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.		Withdrawn from the minimum baseline.	
Control	**Cryptographic Protection**	**Control**	**Cryptographic Protection**
SC-13: Cryptographic Protection The information system implements cryptographic mechanisms, in transit and at rest, validated under the Cryptographic Module Validation Program (see http://csrc.nist.gov/groups/STM/cmvp/validation.html) and in accordance with applicable federal laws, directives, policies, regulations, and standards.		**SC-13: Cryptographic Protection** **a.** Determine the organization-defined cryptographic uses; and **b.** Implement the following types of cryptography required for each specified cryptographic use: at a minimum, the most current FIPS 140-compliant cryptography.	

MARS-E		ARC-AMPE	
Control	**Collaborative Computing Device**	**Control**	**Collaborative Computing Devices and Applications**
SC-15: Collaborative Computing Device The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the organization's CIO or designated representative. If collaborative computing is authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system: **a.** Prohibits remote activation of collaborative computing devices; and **b.** Provides an explicit indication of use to users physically present at the devices. **Implementation Standards** The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.		**SC-15: Collaborative Computing Devices and Applications** **a.** Prohibit remote activation of collaborative computing devices and applications with the following exceptions: no exceptions unless explicitly authorized, in writing, by the organization Chief Information Officer (CIO) or their designated representative; and **b.** Provide an explicit indication of use to users physically present at the devices.	
Control	**Public Key Infrastructure Certificates**	**Control**	**Public Key Infrastructure Certificates**
SC-17: Public Key Infrastructure Certificates The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider. **Implementation Standards** The organization defines the public key infrastructure certificate policy.		**SC-17: Public Key Infrastructure Certificates** **a.** Issue public key certificates under an appropriate certificate policy or obtain public key certificates from an approved service provider; and **b.** Include only approved trust anchors in trust stores or certificate stores managed by the organization.	
Control	**Mobile Code**	**Control**	**Mobile Code**
SC-18: Mobile Code The organization: **a.** Defines acceptable and unacceptable mobile code and mobile code technologies; **b.** Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and **c.** Authorizes, monitors, and controls the use of mobile code within the information system.		**SC-18: Mobile Code** **a.** Define acceptable and unacceptable mobile code and mobile code technologies; and **b.** Authorize, monitor, and control the use of mobile code within the system.	
Control	**Voice Over Internet Protocol**	**Control**	**N/A**
SC-19: Voice Over Internet Protocol The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: **a.** Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously;		Withdrawn control.	

MARS-E		ARC-AMPE	
b. Authorizes, monitors, and controls the use of VoIP within the information system; and **c.** Ensures VoIP equipment used to transmit or discuss sensitive information is protected with CMS (FIPS 140-2 validated module) encryption requirements.			
Control	**Secure Name/Address Resolution Service**	**Control**	**Secure Name/Address Resolution Service (Authoritative Source)**
SC-20: Secure Name/Address Resolution Service The information system: **a.** Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and **b.** Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains when operating as part of a distributed, hierarchical namespace. **Implementation Standards** Recursive lookups are disabled on all publicly accessible domain name system (DNS) servers.		**SC-20: Secure Name/Address Resolution Service (Authoritative Source)** **a.** Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and **b.** Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	
Control	**Secure Name/Address Resolution Service**	**Control**	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**
SC-21: Secure Name/Address Resolution Service The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.		**SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)** Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	
Control	**Architecture and Provisioning for Name/Address Resolution Service**	**Control**	**Architecture and Provisioning for Name/Address Resolution Service**
SC-22: Architecture and Provisioning for Name/Address Resolution Service The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement internal/external role separation.		**SC-22: Architecture and Provisioning for Name/Address Resolution Service** Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	
Control	**Session Authenticity**	**Control**	**Session Authenticity**
SC-23: Session Authenticity The information system protects the authenticity of communications sessions.		**SC-23: Session Authenticity** Protect the authenticity of communications sessions.	
Control	**Protection of Information at Rest**	**Control**	**Protection of Information At Rest**
SC-28: Protection of Information at Rest The information system protects the confidentiality and integrity of information at rest. **a.** The information system protects the confidentiality and integrity of PII.		**SC-28: Protection of Information At Rest** Protect the confidentiality and integrity of all information at rest.	

MARS-E		ARC-AMPE	
Implementation Standards **1.** The information supports the capability to use cryptographic mechanisms to protect information at rest. **2.** In the cloud environment: **a.** The information system enforces encryption of the instance (container) image files under the hypervisor. **b.** Instance (container) image files from virtual server and client deployments must be encrypted in a manner that meets FIPS 140-2 validated requirements.			
Control	**Cryptographic Protection**	**Control**	**Cryptographic Protection**
SC-28 (1): Cryptographic Protection The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the organization's sensitive Information. Organizations must: **a.** Encrypt data at rest in mobile devices for confidentiality to protect against loss, theft, or compromise; **b.** Encrypt data stored in network share drives to insure confidentiality; **c.** Encrypt storage/back-up data where physical protection is either not available, not implemented, or not audited; **d.** If assurance is not provided by other means, encrypt PII in a database; and **e.** Encrypt data stored in the cloud—whether the cloud is government or private. **Implementation Standards** The information system supports the capability to use cryptographic mechanisms to protect information at rest.		**SC-28(01): Cryptographic Protection** Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all organization-defined information at rest.	
Control	**Information System Partitioning**	**Control**	**N/A**
SC-32: Information System Partitioning The organization partitions the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains or environments based on defined circumstances (defined in the applicable security plan) for physical separation of components. **Implementation Standards** When contracting with external service providers, PII, as well as software and services that receive, process, store, or transmit PII, must be isolated within the service provider environment to the maximum extent possible so that other service provider customers sharing physical or virtual space cannot gain access to such data or applications.		Withdrawn from the minimum baseline.	
Control	**Process Isolation**	**Control**	**Process Isolation**
SC-39: Process Isolation The information system maintains a separate execution domain for each executing process.		**SC-39: Process Isolation** Maintain a separate execution domain for each executing process.	
Control	**Electronic Mail**	**Control**	**N/A**

MARS-E	ARC-AMPE
SC-ACA-1: Electronic Mail Controls shall be implemented to protect sensitive information that is sent via email. **Implementation Standards** **1.** Prior to sending an email, place all sensitive information in an encrypted attachment. **2.** Email and any attachment that contains sensitive information when transmitted inside and outside of the organization shall be encrypted using a FIPS 140-2 validated solution. **3.** Password protection of files is recommended to add an additional layer of data protection but shall not be used in lieu of encryption solutions. **4.** Password and/or encryption key shall not be included in the same email that contains sensitive information or in separate email. Password/encryption key shall be provided to the recipient separately via text message, verbally, or other out-of-band solution. **5.** Multi-factor Authentication is required before being granted access to organizational email.	Withdrawn from the minimum baseline.
Control **FAX Usage**	**Control** **N/A**
SC-ACA-2: FAX Usage **a.** If PII is allowed to be included with fax communications, the organization establishes policies and procedures for handling fax transmissions. **b.** The organization must follow specific precautions and Implementation Standards when performing fax transmission of PII: **1.** Transmit PII only to an authorized recipient. **Implementation Standards** **1.** When sending or receiving faxes containing PII: **a.** Fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; **b.** Accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and **c.** A cover sheet must be used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.	Withdrawn from the minimum baseline.

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

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.

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.

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 Communication Protection (SC) 03252025