WHITE PAPER

Migration from EDE to ARC-AMPE System and Information Integrity (SI) controls

CMS requirements for Direct Enrollment Entities

IAN WALTERS, PRINCIPAL
JESSICA PAYNE, CONSULTANT

Table of contents

Purpose

This white paper provides a guide for Direct Enrollment Entities (DEEs) to upgrade their Enhanced Direct Enrollment (EDE) System Security and Privacy Plans (SSPPs) 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 Information Integrity controls.

ARC-AMPE Control Families	
Control Family	**Number of Controls**
Access Control	46
Awareness and Training	9
Audit and Accountability	18
Assessment, Authorization, and Monitoring	12
Configuration Management	25
Contingency Planning	16
Identification and Authentication	21
Incident Response	15
Maintenance	12
Media Protection	8
Physical and Environmental Protection	9
Planning	6
Program Management	5
Personnel Security	8
Personally Identifiable Information Processing and Transparency	10
Risk Assessment	8
System and Services Acquisition	18
System and Communications Protection	28
System and Information Integrity (This Document)	**30**
Supply Chain Risk Management	4

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.

Enhanced Direct Enrollment

> *Direct Enrollment (DE) is a service that allows approved Qualified Health Plan (QHP) issuers and third-party web-brokers (online insurance sellers) to enroll consumers in Exchange coverage, with or without the assistance of an agent/broker, directly from their websites.*
>
> *The Enhanced Direct Enrollment (EDE) user experience goes well beyond the plan shopping and enrollment experience that is available via Classic DE. EDE is a service that allows approved EDE entities (e.g., QHP issuers and web-brokers approved to participate in EDE) to provide a comprehensive consumer experience including the eligibility application, Exchange enrollment, and post-enrollment year-round customer service capabilities for consumers and agents/brokers working on behalf of consumers, directly on issuer and web-broker websites. Through EDE, approved EDE Entities build and host a version of the HealthCare.gov eligibility application directly on their websites that securely integrates with a back-end suite of Federally Facilitated Exchanges (FFEs) application programing interfaces (APIs) to support application, enrollment and more.*
>
> Source: cms.gov

CMS oversight

The Centers for Medicare & Medicaid Services (CMS) exercises oversight of DEEs, 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 DEEs to undergo rigorous audit processes, including demonstrating compliance with security and privacy control requirements.
- Enforcing strict data protection measures in the DE 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 DEEs to adhere to operational policies and procedures, such as providing accurate plan information, maintaining transparent consumer interactions, and facilitating HIM enrollment without bias.
- Requiring DEEs 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 DEEs to renew their Authority to Connect (ATC) annually, providing updated documentation and evidence of continued compliance with all requirements.

Through these oversight mechanisms, CMS ensures that DEEs 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 for Direct Enrollment Entities (DEEs) Version 1.0 dated July 7th, 2025. This framework replaces the EDE 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 DEEs.
- The compliance date for DEEs is June 2026.

The minimum control baseline for ARC-AMPE DEE compliance consists of 308 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 for the mandatory baseline represents a significant increase from the EDE baseline (295 controls), and DEEs should be prepared for an increased level of effort for developing the SSPP and submitting more artifacts during audits.

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

Control mapping

The mapping of the controls found in the EDE audit baseline (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 EDE 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 EDE 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 Information Integrity (SI)

The set of controls in this family focus on how the Exchange shall: (1) identify, report, and correct information and IT system flaws in a timely manner; (2) provide protection from malicious code at appropriate locations within Exchange IT systems; and (3) monitor IT system security alerts and advisories and take appropriate actions in response.

EDE		ARC-AMPE	
Control	**System and Information Integrity Policy and Procedures**	**Control**	**Policy and Procedures**
SI-1: System and Information Integrity Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A system and information integrity 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 information integrity policy and associated system and information integrity controls; and **b.** Reviews and updates (as necessary) the current: **1.** System and information integrity policy at least every three (3) years; and **2.** System and information integrity procedures at least every three (3) years.		**SI-01: Policy and Procedures** **a.** Develop, document, and disseminate to organization-defined personnel or roles: **1.** Organization-level, system, and information integrity 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 information integrity policy and the associated system and information integrity controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and **c.** Review and update the current system and information integrity: **1.** Policy at least every one (1) year and following organization-defined events; and **2.** Procedures at least every one (1) year and following organization-defined events.	
Control	**Flaw Remediation**	**Control**	**Flaw Remediation**
SI-2: Flaw Remediation The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation in a test environment for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates as directed in Implementation Standard 1; and d. Incorporates flaw remediation into the organizational configuration management process. **Implementation Standards** 1. Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days.		**SI-02: Flaw Remediation** **a.** Identify, report, and correct system flaws. **b.** Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; **c.** Install security-relevant software and firmware updates within thirty (30) days of the release of the updates; and **d.** Incorporate flaw remediation into the organizational configuration management process.	

EDE		ARC-AMPE	
a. Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes; and b. Manage the flaw remediation process centrally. 2. A risk-based decision is documented through the configuration management process in the form of written authorization from the organization CIO or his/her designated representative (e.g., the system data owner or organization CISO) and updated documentation in the risk analysis and security plan if a security patch is not to be applied to an information technology component or a legacy (no-longer maintained by the vendor) component is to remain in use. 3. Flaw remediation requirements apply to all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE -identified vulnerability. 4. The organization must provide timely responses, as defined by the CISO, to informational requests for organizational flaw (e.g., patch) status and posture information.			
Control	**Automated Flaw Remediation Status**	**Control**	**Automated Flaw Remediation Status**
SI-2 (2): Automated Flaw Remediation Status The organization employs automated mechanisms no less often than once every seventy-two (72) hours to determine the state of information system components regarding flaw remediation.		**SI-02(02): Automated Flaw Remediation Status** Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms at least monthly.	
Control	**Time to Remediate Flaws / Benchmarks for Corrective Actions**	**Control**	**N/A**
SI-2 (3): Time to Remediate Flaws / Benchmarks for Corrective Actions The organization: a. Measures the time between flaw identification and flaw remediation; and b. Corrective actions must be taken within the time periods defined under the SI-2 (Flaw Remediation) Implementation Standards.		**Withdrawn Control: Incorporated into SI-02**	
Control	**Automated Flaw Remediation Status**	**Control**	**Removal of Previous Versions of Software and Firmware**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**SI-02(06): Removal of Previous Versions of Software and Firmware** Remove previous versions of all upgraded/replaced software and firmware components that are no longer required for operation after updated versions have been installed.	

EDE		ARC-AMPE	
Control	**Malicious Code Protection**	**Control**	**Malicious Code Protection**
SI-3: Malicious Code Protection The organization: **a.** Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; **b.** Updates malicious code protection mechanisms whenever new releases are available in accordance with the organization's configuration management policy and procedures; **c.** Configures malicious code protection mechanisms to: **1.** Perform periodic scans of the information system using the frequency specified in Implementation Standard 1 and Implementation Standard 2, and real-time scans of files from external sources at endpoint, and/or network entry/exit points, as the files are downloaded, opened, or executed in accordance with organizational security policy; and **2.** Block and quarantine malicious code and send alerts to the administrator in response to malicious code detection; and **d.** Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. **Implementation Standards:** **1.** Desktop malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours. **2.** Server (to include databases and applications) malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours. **3.** Malicious code scanning results are reported to the organization Security Information and Event Management (SIEM) team in compliance with AU-6.		**SI-03: Malicious Code Protection** **a.** Implement signature-based and non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; **b.** Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; **c.** Configure malicious code protection mechanisms to: **1.** Perform periodic scans of the system at least every one (1) week and real-time scans of files from external sources at endpoints and network entry and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and **2.** Block and quarantine malicious code and send alert to administrator or organization-defined security personnel near real-time in response to malicious code detection; and **d.** Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	
Control	**Automatic Updates**	**Control**	**N/A**
SI-3 (2): Automatic Updates The information system automatically updates malicious code protection mechanisms.		**Withdrawn Control: Incorporated into SI-3.**	
Control	**Information System Monitoring**	**Control**	**System Monitoring**
SI-4: Information System Monitoring The organization: **a.** Monitors the information system to detect: **1.** Attacks and indicators of potential attacks in accordance with the current organizational incident handling policy and procedures; and **2.** Unauthorized local, network, and remote connections twice weekly;		**SI-04: System Monitoring** **a.** Monitor the system to detect: **1.** Attacks and indicators of potential attacks in accordance with the following monitoring objectives: organization's incident response policy and procedures (refer to IR-1); and **2.** Unauthorized local, network, and remote connections;	

EDE	ARC-AMPE
b. Identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable System Security Plan); **c.** Deploys monitoring devices: **1.** Strategically within the information system to collect organization-determined essential information; and **2.** At ad hoc locations within the system to track specific types of transactions of interest to the organization. **d.** Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; **e.** Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, and other organizations based on law enforcement information or other credible sources of information; **f.** Obtains legal opinion about information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and **g.** Provides defined information system monitoring information (defined in the applicable System Security Plan) to defined personnel or roles (defined in the applicable System Security Plan) as needed, and at defined frequency (defined in the applicable System Security Plan). **Implementation Standards** **1.** Implement a centrally managed Intrusion Detection System/Intrusion Protection System (IDS/IPS) capability to monitor network communications on all networks and subnets of any environment requiring an organization Authority to Operate. **a.** Permitted IDS/IPS mechanisms: • Centrally managed IDS/IPS devices at network perimeter points, to include between zones; and • Centrally managed host-based IDS/IPS sensor agents in information technology components for which such agents are available. **b.** Environments where communications within the zone are encrypted must use mechanisms capable of either decrypting content for analysis or analyzing content before transmission/after receipt; and **c.** Information technology components that do not support host-based IDS/IPS sensors capability must be documented in the applicable risk assessment and security plan. **2.** Monitoring functionality supports the sharing of threat awareness information in a format that meets organizational requirements. **3.** The organization monitors for unauthorized remote connections to the information system continuously, in real time and takes appropriate action if an unauthorized connection is discovered.	**b.** Identify unauthorized use of the system through the following techniques and methods: organization-defined techniques and methods documented in the applicable System Security and Privacy Plan (SSPP); **c.** Invoke internal monitoring capabilities or deploy monitoring devices: **1.** Strategically within the system to collect organization-determined essential information; and **2.** At ad hoc locations within the system to track specific types of transactions of interest to the organization; **d.** Analyze detected events and anomalies; **e.** Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; **f.** Obtain legal opinion regarding system monitoring activities; and **g.** Provide organization-defined system monitoring information to organization-defined personnel or roles as needed and consistent with the organization-defined frequency documented in the applicable System Security and Privacy Plan (SSPP).

EDE		ARC-AMPE	
Control	**System-Wide Intrusion Detection System**	**Control**	**System-Wide Intrusion Detection System**
SI-4 (1): System-Wide Intrusion Detection System The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.		**SI-04(01): System-Wide Intrusion Detection System** Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	
Control	**Inbound and Outbound Communications Traffic**	**Control**	**Inbound and Outbound Communications Traffic**
SI-4 (4): Inbound and Outbound Communications Traffic The information system monitors inbound and outbound communications traffic at a defined frequency (defined in the applicable security plan) for unusual or unauthorized activities or conditions.		**SI-04(04): Inbound and Outbound Communications Traffic** **a.** Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; **b.** Monitor inbound and outbound communications traffic continuously for organization-defined unusual or unauthorized activities or conditions.	
Control	**System-Generated Alerts**	**Control**	**System-Generated Alerts**
SI-4 (5): System-Generated Alerts The information system sends alerts to defined personnel or roles (defined in the applicable security plan) when the following indications of compromise or potential compromise occur: **a.** Presence of malicious code; **b.** Unauthorized export of information; **c.** Signaling to an external information system; or **d.** Potential intrusions. **Implementation Standards:** **1.** The organization defines additional compromise indicators as needed. **2.** The indications that a compromise or potential compromise occurred include: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline configuration/system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.		**SI-04(05): System-Generated Alerts** Alert organization-defined personnel or roles when the following system-generated indications of compromise or potential compromise occur: presence of malicious code, unauthorized export of information, signaling to an external information system, or potential intrusions.	

EDE		ARC-AMPE	
Control	**N/A**	**Control**	**Host-Based Devices**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**SI-04(23): Host-Based Devices** Implement the following host-based monitoring mechanisms at organization system components: intrusion detection system / intrusion prevention system (IDS/IPS).	
Control	**Security Alerts, Advisories, and Directives**	**Control**	**Security Alerts, Advisories, and Directives**
SI-5: Security Alerts, Advisories, and Directives The organization: **a.** Receives information system security alerts, advisories, and directives from defined external organizations (including US-CERT and organizations as defined in the applicable System Security Plan) on an ongoing basis; **b.** Generates internal security alerts, advisories, and directives as deemed necessary; **c.** Disseminates security alerts, advisories, and directives to: defined personnel or roles (defined in the applicable System Security Plan); **d.** The organization defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives; and **e.** Implements security directives in accordance with established time frames or notifies the Authorizing Official of the degree of noncompliance.		**SI-05: Security Alerts, Advisories, and Directives** **a.** Receive system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis; **b.** Generate internal security alerts, advisories, and directives as deemed necessary; **c.** Disseminate security alerts, advisories, and directives to, at a minimum, system security personnel and administrators with configuration / patch-management responsibilities; and **d.** Implement security directives in accordance with established timeframes, or notify the issuing organization of the degree of noncompliance.	
Control	**Security Function Verification**	**Control**	**Security and Privacy Function Verification**
SI-6: Security Function Verification The information system: **a.** Verifies the correct operation of defined security functions (defined in the applicable System Security Plan); **b.** Performs this verification upon system startup, restart, and upon command by a user with appropriate privileges no less often than once per month; **c.** Notifies the system administrators of failed security verification tests; and **d.** Shuts the information system down, or restarts the information system, or performs some other defined alternative action(s) (defined in the applicable System Security Plan) when anomalies are discovered.		**SI-06: Security and Privacy Function Verification** **a.** Verify the correct operation of organization-defined security and privacy functions; **b.** Perform the verification of the functions specified in SI-6a upon system startup and/or restart, upon command by a user with appropriate privileges, or at least monthly; **c.** Alert, at a minimum, the system / security administrator to failed security and privacy verification tests; and **d.** Shut the system down, restart the system, or perform another defined alternative action(s) documented in the applicable System Security and Privacy Plan (SSPP) when anomalies are discovered.	
Control	**Software, Firmware, and Information Integrity**	**Control**	**Software, Firmware, and Information Integrity**
SI-7: Software, Firmware, and Information Integrity The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.		**SI-07: Software, Firmware, and Information Integrity** **a.** Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: organization-defined software, firmware, and information; and **b.** Take the following actions when unauthorized changes to the software, firmware, and information are detected: include such organization-defined actions as parity checks, cyclical redundancy checks, and cryptographic hashes.	

EDE		ARC-AMPE	
Control	**Integrity Checks**	**Control**	**Integrity Checks**
SI-7 (1): Integrity Checks The organization performs an integrity check of software, firmware, and information daily and at system startup and reassesses the integrity of software and information by performing no less often than one monthly scan of the information system.		**SI-07(01): Integrity Checks** Perform an integrity check of organization software, firmware, and information at startup, at transitional states or security-relevant events, and at least monthly.	
Control	**Integration of Detection and Response**	**Control**	**Integration of Detection and Response**
SI-7 (7): Integration of Detection and Response The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.		**SI-07(07): Integration of Detection and Response** Incorporate the detection of the following unauthorized changes into the organizational incident response capability: organization-defined security-relevant changes to the system to include unauthorized changes to established organizational configuration settings and the unauthorized elevation of system privileges.	
Control	**Spam Protection**	**Control**	**Spam Protection**
SI-8: Spam Protection The organization: **a.** Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and **b.** Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.		**SI-08: Spam Protection** **a.** Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and **b.** Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	
Control	**Automatic Updates**	**Control**	**Automatic Updates**
SI-8 (2): Automatic Updates The information system automatically updates spam protection mechanisms.		**SI-08(02): Automatic Updates** Automatically update spam protection mechanisms at least every one (1) week.	
Control	**Information Input Validation**	**Control**	**Information Input Validation**
SI-10: Information Input Validation The information system checks the validity of defined information inputs (defined in the System Security Plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible and the validity of personally identifiable information (PII) being processed, stored, or transmitted.		**SI-10: Information Input Validation** Check the validity of the following information inputs: all inputs to web / application servers, database servers, and any system or application input that might receive a crafted exploit toward executing some code or buffer overflow.	
Control	**Error Handling**	**Control**	**Error Handling**
SI-11: Error Handling The information system: a. Generates error messages that provide information necessary for corrective actions without revealing user name and password combinations; attributes used to validate a password reset request (e.g., security questions); personally identifiable information		**SI-11: Error Handling** **a.** Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and **b.** Reveal error messages only to organization-defined personnel or roles documented in the applicable System Security and Privacy Plan (SSPP).	

EDE		ARC-AMPE	
(excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings in error logs and administrative messages that could be exploited by adversaries.; and b. Reveals error messages only to defined personnel or roles (defined in the System Security Plan). c. Reveals error messages only to authorized individuals with a need for the information in the performance of their duties.			
Control	**Information Handling and Retention**	**Control**	**Information Management and Retention**
SI-12: Information Handling and Retention The organization handles and retains information within the information system and information output from the system in accordance with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. **Implementation Standard** Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system for ten (10) years or in accordance with organizational requirements, whichever is more restrictive.		**SI-12: Information Management and Retention** Manage and retain information within the system and information output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines and operational requirements.	
Control	**N/A**	**Control**	**Limit Personally Identifiable Information Elements**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-12(01): Limit Personally Identifiable Information Elements** Limit Personally Identifiable Information (PII) processed in the information life cycle to the minimum PII elements that are necessary to accomplish the legally authorized purpose of collection.	
Control	**N/A**	**Control**	**Minimize Personally Identifiable Information in Testing, Training, and Research**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-12(02): Minimize Personally Identifiable Information in Testing, Training, and Research** Use techniques in accordance with organizational standards and applicable federal and state laws and regulations to minimize the use of Personally Identifiable Information (PII) for research, testing, or training.	
Control	**N/A**	**Control**	**Information Disposal**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-12(03): Information Disposal** Use the following techniques to dispose of, destroy, or erase information following the retention period: organization-defined	

EDE		ARC-AMPE	
		techniques and in a manner that prevents loss, theft, misuse, or unauthorized access.	
Control	**Memory Protection**	**Control**	**Memory Protection**
SI-16: Memory Protection The information system implements security safeguards (e.g., data execution prevention and address space layout randomization) to protect its memory from unauthorized code execution. Implemented safeguards must be specified in the applicable system security plan.		**SI-16: Memory Protection** Implement the following controls to protect the system memory from unauthorized code execution: at a minimum, the related control controls within this control set.	
Control	**N/A**	**Control**	**Personally Identifiable Information Quality Operations**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-18: Personally Identifiable Information Quality Operations** **a.** Check the accuracy, relevance, timeliness, and completeness of Personally Identifiable Information (PII) across the information life cycle at least every one (1) year; and **b.** Correct or delete inaccurate or outdated PII.	
Control	**N/A**	**Control**	**Individual Requests**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-18(04): Individual Requests** Correct or delete Personally Identifiable Information (PII) upon request by individuals or their designated representatives.	
Control	**N/A**	**Control**	**Notice of Collection or Deletion**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-18(05): Notice of Collection or Deletion** Notify organization-defined authorized recipients of Personally Identifiable Information (PII) and individuals whose PII has been corrected or deleted.	
Control	**N/A**	**Control**	**De-Identification**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-12: De-Identification** **a.** Remove the following elements of Personally Identifiable Information (PII) from datasets: organization-defined elements of PII as required by laws, policies, or regulations, as needed for relevant functions; and **b.** Evaluate every one (1) year for effectiveness of de-identification.	
Control	**N/A**	**Control**	**Release**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-19(03): Release** Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	

EDE		ARC-AMPE	
Control	**N/A**	**Control**	**Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**SI-19(04): Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers** Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	

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**.

WP_ACA CMS Controls Migration (System and Information Integrity (SI)_07142025