NIST 800-53+ Moderate System Controls

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Cntl #	Required Control	Risk
RA-00	***1.1 Risk Assessment (RA) Family***	
RA-01	**1.1.1 RA-1 – Risk Assessment P&P [M]** *[NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*	
RA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
RA-01a	a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
RA-01b	b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	L
RA-02	**1.1.2 RA-2 – Security Categorization [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
RA-02a	The organization shall: a. Categorize information and the information system in accordance with applicable federal standards and guidance.	M
RA-02b	b. Document the security categorization results (including supporting rationale) in the security plan for the information system.	M
RA-02c	c. Ensure the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	M
RA-03	**1.1.3 RA-3 – Risk Assessment [M]** *[NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*	

Cntl #	Required Control	Risk
RA-03a	The organization shall: a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.	M
RA-03b	b. Document risk assessment results.	M
RA-03c	c. Review risk assessment results within every three-hundred-sixty-five (365) days.	M
RA-03d	d. Update the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.	M
RA-03e	e. *[ISO 27001:2005]* Events/Scenarios that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	M
RA-03m	[Medicaid Information Technology Architecture] f. The threat modeling process shall consist of the following steps: i. Identify assets along a service value chain and define the roles and required privileges of persons involved in delivering that service. ii. Create a Service Architecture Delivery Model for each service channel. iii. Decompose the service application and annotate with S&P integration points. iv. Identify threats (a list of standard threats exists, but many applications can introduce new threats). v. Document threats by gathering them into the recommended threat tool. vi. Rate threats by using a risk rating based on asking the following questions: • How much damage can be done if someone exploited the vulnerability? (Damage Potential) • How easily can someone reproduce the attack? (Reproducibility) • How easily can someone launch an attack? (Exploitability) • Approximately how many users does it affect? (Affected Users) • How easily can someone find the vulnerability? (Discoverability) vii. Perform multi-criteria countermeasure analysis. viii. Summarize residual threats.	M
RA-05	**1.1.4 RA-5 – Vulnerability Scanning [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
RA-05a	The organization shall: a. Scan for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported.	M
RA-05b	b. Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: i. Enumerating platforms, software flaws, and improper configurations. ii. Formatting and making transparent, checklists and test procedures. iii. Measuring vulnerability impact.	M
RA-05c	c. Analyze vulnerability scan reports and results from security control assessments.	M
RA-05d	d. Remediate legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk.	M
RA-05e	e. Share information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	M
RA-05f	f. Employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	M
RA-99	This line is a blank spacer line.	

Cntl #	Required Control	Risk
PL-00	## *1.2 Planning (PL) Family*	
PL-01	### 1.2.1 PL-1 – Security Planning P&P [M] *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PL-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
PL-01a	a. A formal, documented security planning **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
PL-01b	b. Formal, documented **procedures** to facilitate the implementation of the security planning policy and associated security planning controls.	L
PL-02	### 1.2.2 PL-2 – System Security Plan (SSP) [M] *[NIST 800-53, CMS MARS-E, IRS 1075]*	
PL-02a	The organization shall: a. **Develop a security plan for the information system** that: i. Is consistent with the **ACA System Security Plan (SSP) Procedure**. ii. Is consistent with the State's enterprise architecture. iii. Explicitly defines the authorization boundary for the system. iv. Describes the operational context of the system in terms of missions and business processes. v. Describes the operational environment for the system. vi. Describes relationships with or connections to other information systems. vii. Provides an overview of the security requirements for the system. viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions. ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.	M
PL-02b	b. Review the security plan for the information system within every three-hundred-sixty-five (365) days.	M
PL-02c	c. Update the plan, minimally every three (3) years, to address current conditions or whenever: i. There are significant changes to the system/environment of operation that affect security. ii. Problems are identified during plan implementation or security control assessments. iii. When the data sensitivity level increases. iv. After a serious security violation due to changes in the threat environment. v. Before the previous security authorization expires.	M
PL-04	### 1.2.3 PL-4 – Rules of Behavior (ROB) [M] *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PL-04a	The organization shall: a. Establish and make readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information, information system, and network use.	M
PL-04b	b. Receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	M
PL-04c	c. ***[IRS 1075]*** The agency shall promulgate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules shall address brief absences while employees are away from the computer.	M

Cntl #	Required Control	Risk
PL-05	**1.2.4 PL-5 – Privacy Impact Assessment (PIA) [M]** *[NIST 800-53, CMS MARS-E]*	
PL-05a	a. The organization shall conduct a Privacy Impact Assessment (PIA) in accordance with OMB policy M-03-22.	M
PL-06	**1.2.5 PL-6 – Security-Related Activity Planning [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PL-06a	a. The organization shall plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on operations (i.e., mission, functions, image, and reputation), assets, and individuals.	M
PL-99	This is a blank formatting row.	
SA-00	***1.3 System and Services Acquisition (SA)***	
SA-01	**1.3.1 SA-1 – System& Services Acquisition P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
SA-01a	a. A formal, documented system and services acquisition **policy** that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
SA-01b	b. Formal, documented **procedures** to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	L
SA-02	**1.3.2 SA-2 – Allocation of Resources [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SA-02a	The organization shall: a. Include a determination of information security requirements for the information system in mission/business process planning.	M
SA-02b	b. Determine, document, and allocate the resources required to protect the information system as part of its capital planning and investment control process.	M
SA-02c	c. Include information security requirements in mission/business case planning.	M
SA-02d	d. Establish a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.	M
SA-03	**1.3.3 SA-3 – Life Cycle Support [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SA-03a	The organization shall: a. Manage the lifecycle of the information system.	M
SA-03b	b. Define and document information system security roles and responsibilities throughout the system development life cycle.	M
SA-03c	c. Identify individuals having information system security roles and responsibilities.	M

Cntl #	Required Control	Risk
SA-04	**1.3.4 SA-4 – Acquisitions [M]** *[NIST 800-53, CMS MARS-E]*	
SA-04a	a. The organization shall include the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: i. Security functional requirements/specifications. ii. Security-related documentation requirements. iii. Developmental and evaluation-related assurance requirements.	M
SA-04b	b. The organization shall require in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.	M
SA-04c	c. The organization shall ensure that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	M
SA-04.1	Describe how the organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system.	
SA-04.4	Describe how the organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	
SA-05	**1.3.5 SA-5 – System Documentation [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
SA-05a	The organization shall: a. Obtain, protect as required, and make available to authorized personnel, administrator documentation for the information system that describes: i. Secure configuration, installation, and operation of the information system. ii. Effective use and maintenance of security features/functions. iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.	M
SA-05b	b. Obtain, protect as required, and make available to authorized personnel, user documentation for the information system that describes: i. User-accessible security features/functions and how to effectively use those security features/functions. ii. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner. iii. User responsibilities in maintaining the security of the information and information system.	M
SA-05c	c. Document attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	M
SA-05d	d. Obtain, protect as required, and make available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.	M

Cntl #	Required Control	Risk
SA-05e	e. Obtain, protect as required, and make available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	M
SA-06	**1.3.6 SA-6 – Software Usage Restrictions [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
SA-06a	The organization shall: a. Use software and associated documentation in accordance with contract agreements and copyright laws.	M
SA-06b	b. Employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.	M
SA-06c	c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	M
SA-07	**1.3.7 SA-7 – User-Installed Software [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
SA-07a	a. The organization shall prohibit users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users.	M
SA-08	**1.3.8 SA-8 – Security Engineering Principles [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SA-08a	a. The organization shall apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	M
SA-09	**1.3.9 SA-9 – External System Services [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, SSA System Security Guidelines]*	
SA-09a	The organization shall prohibit service providers from outsourcing any system function outside the U.S. or its territories. If authorized the organization shall: a. Require 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.	M
SA-09b	b. Define and document oversight and user roles and responsibilities with regard to external information system services.	M
SA-09c	c. Ensure that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.	M
SA-09d	d. Monitor security control compliance by external service providers.	M
SA-09e	e. ***[ISO 27001:2005]*** The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	M

Cntl #	Required Control	Risk
SA-09f	f. Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	M
SA-09bg	g. The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.	M
SA-10	**1.3.10 SA-10 – Developer Configuration Mgmt [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
SA-10a	The organization shall require that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation.	M
SA-10b	b. Manage and control changes to the information system.	M
SA-10c	c. Implement only organization-approved changes.	M
SA-10d	d. Document approved changes to the information system.	M
SA-10e	e. Track security flaws and flaw resolution.	M
SA-11	**1.3.11 SA-11 – Developer Security Testing [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SA-11a	The organization shall require that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan in accordance with, but not limited to the, current procedures.	M
SA-11b	b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process.	M
SA-11c	c. Document the results of the security control assessment and flaw remediation processes.	M
SA-11d	*[ISO 27001:2005]* d. Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.	M
SA-99	This line is a blank spacer line.	
CA-00	***1.4 Security Assessment and Authorization (CA) Family***	
CA-01	**1.4.1 CA-1 – Security Assessment and Authorization P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
CA-01a	a. Formal, documented security assessment and authorization **policies** that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
CA-01b	b. Formal, documented **procedures** to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	L

Cntl #	Required Control	Risk
CA-02	**1.4.2 CA-2 – Security Assessments [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
CA-02a	The organization shall: a. Develop a security assessment plan that describes the scope of the assessment including: i. Security controls and control enhancements under assessment. ii. Assessment procedures to be used to determine security control effectiveness. iii. Assessment environment, assessment team, and assessment roles and responsibilities.	M
CA-02b	b. Assess the security controls in the information system within every three-hundred-sixty-five (365) days to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	M
CA-02c	c. Produce a security assessment report that documents the results of the assessment.	M
CA-02d	d. Provide the results of the security control assessment within every three-hundred-sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.	M
CA-02e	e. Employ an independent assessor or assessment team to conduct an assessment of the security controls.	M
CA-03	**1.4.3 CA-3 – Information System Connections [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CA-03a	The organization shall: a. Authorize connections to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements.	M
CA-03b	b. Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.	M
CA-03c	c. Monitor the information system connections on an ongoing basis verifying enforcement of security requirements.	M
CA-03d	d. *[ISO 27001:2005]* Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.	M
CA-05	**1.4.4 CA-5 – Plan of Action and Milestones [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CA-05a	The organization shall: a. Develop and submit a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	M
CA-05b	b. Update and submit existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	M

Cntl #	Required Control	Risk
CA-05c	[CMS MARS-E] c. The organization shall employ automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.	M
CA-06	**1.4.5 CA-6 – Security Authorization [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
CA-06a	a. Explicit authorization to operate the information system shall be received from the CMS CIO or his/her designated representative prior to the system being placed into operations. If the authorization is an interim approval to operate, then the authorization shall be granted based on the designated security category of the information system. An explicit corrective action plan shall be developed, implemented effectively, and monitored by the authorizing official.	M
CA-06b	b. The organization shall update the security authorization: i. At least every three (3) years. ii. When substantial changes are made to the system. iii. When changes in requirements result in the need to process data of a higher sensitivity. iv. When changes occur to authorizing legislation or federal requirements. v. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization. vi. Prior to expiration of a previous security authorization.	M
CA-07	**1.4.6 CA-7 – Continuous Monitoring [M]** *[NIST 800-53, The Patient Protection and Affordable Care Act, CMS MARS-E, IRS 1075]*	
CA-07a	a. The organization shall establish a continuous monitoring strategy and implement a continuous monitoring program that includes:	M
CA-07a1	i. A configuration management process for the information system and its constituent components.	M
CA-07a2	ii. A determination of the security impact of changes to the information system and environment of operation.	M
CA-07a3	iii. Ongoing security control assessments in accordance with **the organizational continuous monitoring strategy.**	M
CA-07a4	iv. Reporting the security state of the information system to appropriate organizational officials within every three-hundred-sixty-five (365) days.	M
CA-07.1	**The use of independent security assessment agents or teams to monitor security controls is not required**. However, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.	M
CA-07.2	Describe how the organization plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all information systems and information systems that are processing data on behalf of or directly for including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.	M
CA-99	This is a blank formatting row.	
PM-00	***1.5 Information Security Program Management (PM) Family***	

Cntl #	Required Control	Risk
PM-01	**1.5.1 PM-1 Information Security Program Plan** *[NIST 800-53, CMS MARS-E]*	
PM-01a	The organization shall: a. Develop and disseminate an organization-wide information **security program plan** that: i. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements. ii. Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. iii. Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance. iv. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.	M
PM-01b	b. Review the organization-wide information security program plan at an organization defined frequency.	M
PM-01c	c. Revise the plan to address organizational changes and problems identified during plan implementation or security control assessments.	M
PM-02	**1.5.2 PM-2 Senior Information Security Officer** *[NIST 800-53, CMS MARS-E]*	
PM-02a	a. The organization shall appoint a senior information security officer with the mission and **resources** to coordinate, develop, implement, and maintain an organization-wide information security program.	M
PM-03	**1.5.3 PM-3 Information Security Resources** *[NIST 800-53, CMS MARS-E]*	
PM-03a	The organization shall: a. **Ensure that all capital planning and investment requests include the resources needed to implement the information security program** and document all exceptions to this requirement.	M
PM-03b	b. Employ a business case/Exhibit 300/Exhibit 53 to record the resources required.	M
PM-03c	c. Ensure that information security resources are available for expenditure as planned.	M
PM-04	**1.5.4 PM-4 Plan Of Action And Milestones Process** *[NIST 800-53, CMS MARS-E]*	
PM-04a	a. The organization shall implement a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	M
PM-05	**1.5.5 PM-5 Information System Inventory** *[NIST 800-53, CMS MARS-E]*	

Cntl #	Required Control	Risk
PM-05a	a. The organization shall develop and maintain an inventory of its information systems.	M
PM-06	**1.5.6 PM-6 Info. Security Measures of Performance** *[NIST 800-53, CMS MARS-E]*	
PM-06a	a. The organization shall develop, monitor, and report on the results of information security measures of performance.	M
PM-07	**1.5.7 PM-7 Enterprise Architecture** *[NIST 800-53, CMS MARS-E]*	
PM-07a	a. The organization shall develop enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	M
PM-08	**1.5.8 PM-8 Critical Infrastructure Plan** *[NIST 800-53, CMS MARS-E]*	
PM-08a	a. The organization shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	M
PM-09	**1.5.9 PM-9 Risk Management Strategy** *[NIST 800-53, CMS MARS-E]*	
PM-09a	The organization shall: a. Develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.	M
PM-09b	b. Implement that strategy consistently across the organization.	M
PM-10	**1.5.10 PM-10 Security Authorization Process**	
PM-10a	a. The organization: manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;	M
PM-10b	b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and	M
PM-10c	c. Fully integrates the security authorization processes into an organization-wide risk management program.	M
PM-10d	***Supplemental Guidance**: The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.*	
PM-11	**1.5.11 PM-11 Mission/Business Process Definition**	
PM-11a	The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and	M
PM-11b	b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	M

Cntl #	Required Control	Risk
PM-11c	***Supplemental Guidance**: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.*	M
PM-99	This is a blank formatting line.	
IA-00	## *1.6 Identification and Authentication (IA)*	
IA-01	### 1.6.1 IA-1 – Identification& Authentication P&P [M] *[NIST 800-53, CMS MARS-E, IRS 1075]*	
IA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
IA-01a	a. A formal, documented identification and authentication **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
IA-01b	b. Formal, documented **procedures** to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	L
IA-02	### 1.6.2 IA-2 – Identification and Authentication (Org. Users) [M] *[NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
IA-02a	The information system shall: a. Uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	M
IA-02b	b. Use **multifactor authentication** for network access to privileged accounts.	M
IA-02c	c. Use **multifactor authentication** for network access to non-privileged accounts.	M
IA-02d	d. Use **multifactor authentication** for local access to privileged accounts.	M
IA-02e	**e. Use replay resistant authentication mechanisms for network access to privileged accounts.**	M
IA-02f	f. *[IRS 1075]* The agency shall configure the web services to be authenticated before access is granted to users via an authentication server. The web portal and 2-factor authentication requirements apply in a data warehouse environment. Business roles and rules shall be imbedded at either the authentication level or application level. Authentication shall be required both at the operating system level and at the application level, when accessing the data warehousing environment.	M
IA-03	### 1.6.3 IA-3 – Device Identification and Authentication [M] *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
IA-03a	a. The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection.	M

Cntl #	Required Control	Risk
IA-04	**1.6.4 IA-4 – Identifier Management [M]** *[NIST 800-53, CMS MARS-E]*	
IA-04a	The organization shall manage information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier.	M
IA-04b	b. Selecting an identifier that uniquely identifies an individual or device.	M
IA-04c	c. Assigning the user identifier to the intended party or the device identifier to the intended device.	M
IA-04d	d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired.	M
IA-04e	e. Disabling the user identifier after sixty (60) days or less and deleting disabled accounts during the annual re-certification process.	M
IA-05	**1.6.5 IA-5 – Authenticator Management [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]*	
IA-05a	The organization shall manage information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.	M
IA-05b	b. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.	M
IA-05c	*[NIST 800-53, CMS MARS-E, IRS 1075]* c. The information system, for password-based authentication shall: i. Automatically force users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days. *ii.* ***[IRS 1075]*** *Prohibit the use of dictionary words, popular phrases, or obvious combinations of letters and numbers in passwords shall be prohibited when possible. Obvious combinations of letters and numbers include first names, last names, initials, pet names, user accounts spelled backwards, repeating characters, consecutive numbers, consecutive letters, and other predictable combinations and permutations.* iii. Enforce minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters. iv. Enforce at least a minimum of four (4) changed characters when new passwords are created. v. Encrypt passwords in storage and in transmission. vi. Enforce password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum. vii. Prohibit password reuse for six (6) generations prior to reuse.	M
IA-05d	d. The information system, for PKI-based authentication shall: i. Validate certificates by constructing a certification path with status information to an accepted trust anchor. ii. Enforce authorized access to the corresponding private key. iii. Map the authenticated identity to the user account.	M
IA-05e	e. The organization shall require that the registration process to receive hardware tokens be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	M

Cntl #	Required Control	Risk
IA-05f	***[IRS 1075]*** f. Passwords shall be systematically disabled after 90 days of inactivity to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods.	M
IA-05g	g. Users shall be prohibited from changing their passwords for at least 15 days after a recent change. Meaning, the minimum password age limit shall be 15 days after a recent password change.	M
IA-05h	h. Privileged users shall be able to override the minimum password age limit for users when necessary to perform required job functions.	M
IA-05i	i. The information system shall routinely prompt users to change their passwords within 5-14 days before such password expires.	M
IA-05j	j. User account lockout feature shall disable the user account after 3 unsuccessful login attempts.	M
IA-05k	k. Account lockout duration shall be permanent until an authorized system administrator reinstates the user account.	M
IA-05l	l. Default vendor passwords shall be changed upon successful installation of the information system product.	M
IA-05m	m. System initialization (boot) settings shall be password-protected.	M
IA-05n	n. Clear-text representation of passwords shall be suppressed (blotted out) when entered at the login screen.	M
IA-05o	o. Passwords shall not be automated through function keys, scripts or other methods where passwords may be stored on the system.	M
IA-05p	p. Users shall commit passwords to memory, avoid writing passwords down and never disclose passwords to others (e.g., with a co-worker in order to share files).	M
IA-06	**1.6.6 IA-6 – Authenticator Feedback [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
IA-06a	a. The information system shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	M
IA-07	**1.6.7 IA-7 – Cryptographic Module Authent. [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
IA-07a	a. The information system shall use mechanisms for **authentication to a cryptographic module** that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	M
IA-08	**1.6.8 IA-8 – Identification and Authentication (Non-Organizational Users) [M]** *[NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]*	
IA-08a	a. The information system shall uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	M
IA-99	This is a blank formatting line.	
AC-00	***1.7 AC – Access Control***	

Cntl #	Required Control	Risk
AC-01	**1.7.1 AC-1 – Access Control P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
AC-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
AC-01a	a. A formal, documented access control **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
AC-01b	b. Formal, documented **procedures** to facilitate the implementation of the access control policy and associated access controls.	L
AC-02	**1.7.2 AC-2 – Account Management [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
AC-02a	a. The organization shall manage information system accounts, including:	M
AC-02a1	i. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary).	M
AC-02a2	ii. Establishing conditions for group membership.	M
AC-02a3	iii. Identifying authorized users of the information system and specifying access privileges.	M
AC-02a4	iv. Requiring appropriate approvals for requests to establish accounts.	M
AC-02a5	v. Establishing, activating, modifying, disabling, and removing accounts.	M
AC-02a6	vi. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts.	M
AC-02a7	vii. Notifying account managers when temporary accounts are no longer required and when information system users are terminated transferred, or information system usage or need-to-know/need-to-share changes.	M
AC-02a8	viii. Deactivating: (a) temporary accounts that are no longer required (not to exceed three-hundred sixty-five (365) days); (b) inactive accounts after an organization-defined time period; and (c) accounts of terminated or transferred users.	M
AC-02a9	ix. Terminating emergency accounts within twenty-four (24) hours.	M
AC-02a10	x. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions.	M
AC-02a11	xi. Reviewing information system accounts within every one-hundred-eighty (180) days and requiring annual certification.	M
AC-02a12	xii. Automatically audit account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	M
AC-02.1	The organization employs automated mechanisms to support the management of information system accounts.	M
AC-02.2	The information system automatically terminates emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three hundred sixty-five (365) days.	M
AC-02.3	The information system automatically disables inactive accounts after one hundred eighty (180) days.	M
AC-02.4	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	M

Cntl #	Required Control	Risk
AC-02.7a	The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;	M
AC-02.7b	b. Tracks and monitors privileged role assignments; and Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.	M
AC-02.7c	c. Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.	M
AC-03	**1.7.3 AC-3 – Access Enforcement [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075, IRS Pub 3373 DIFSLA, SSA SysSec Guidelines]*	
AC-03a	a. The information system shall enforce approved authorizations for logical access to the system in accordance with applicable policy.	M
AC-03b	[SSA System Security Guidelines] The organization shall use a recognized user access security software package (e.g. RAC-F, ACF-2, and TOP SECRET) or an equivalent security software design. The access control software shall utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system.	M
AC-04	**1.7.4 AC-4 – Information Flow Enforcement [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AC-04a	a. The information system shall enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	M
AC-04b	b. *[ISO 27001:2005]* Groups of information services, users, and information systems shall be segregated on networks.	M
AC-04c	c. Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	M
AC-04d	d. Opportunities for information leakage shall be prevented.	M
AC-05	**1.7.5 AC-5 – Separation of Duties [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
AC-05a	The organization shall: a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.	M
AC-05b	b. Document separation of duties.	M
AC-05c	c. Implement separation of duties through assigned information system access authorizations.	M
AC-06	**1.7.6 AC-6 – Least Privilege [M]** *[NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075, SSA System Security Guidelines]*	
AC-06a	The organization shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with system missions and business functions.	M
AC-06.1	The organization explicitly authorizes access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.	M

Cntl #	Required Control	Risk
AC-06.2	The organization requires that users of information system accounts, or roles, with access to administrator accounts or security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions	M
AC-07	**1.7.7 AC-7 – Unsuccessful Login Attempts [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
AC-07a	The information system shall: a. Enforce the limit of consecutive invalid login attempts by a user to three (3) during a fifteen (15) minute time period.	M
AC-07b	b. Automatically disable or lock the account/node for thirty (30) minutes until released when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	M
AC-08	**1.7.8 AC-8 – System Use Notification [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
AC-08a	The information system shall: a. Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner for information systems shall be: • You are accessing a U.S. State information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. • Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. • By using this information system, you understand and consent to the following: * You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. * Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.	M
AC-08b	b. Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information system.	M
AC-08c	c. For publicly accessible systems: (i) display the system use information when appropriate, before granting further access; (ii) display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) include in the notice given to public users of the information system, a description of the authorized uses of the system.	M
AC-10	**1.7.9 AC-10 – Concurrent Session Control [M]** *[NIST 800-53, CMS MARS-E]*	

Cntl #	Required Control	Risk
AC-10a	a. The information system shall limit the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions shall be limited and enforced to the number of sessions expressly required for the performance of job duties and requirement for more than one (1) concurrent application/process session shall be documented in the security plan. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.	M
AC-11	**1.7.10 AC-11 – Session Lock [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
AC-11a	The information system shall: a. Prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity.	M
AC-11b	b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.	M
AC-14	**1.7.11 AC-14 – Permitted Actions without Identification or Authentication [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AC-14a	a. The organization shall document and provide supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	M
AC-14b	b. Configure Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.	M
AC-14c	c. Permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	M
AC-17	**1.7.12 AC-17 – Remote Access [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
AC-17	**Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and shall be explicitly authorized, in writing, by the CIO or his/her designated representative.**	M
AC-17a	**If authorized**, the organization shall: a. Document allowed methods of remote access to the information system.	M
AC-17b	b. Establish usage restrictions and implementation guidance for each allowed remote access method.	M
AC-17c	c. Monitor for unauthorized remote access to the information system.	M
AC-17d	d. Authorize remote access to the information system prior to connection.	M
AC-17e	e. Enforce requirements for remote connections to the information system.	M
AC-17f	[NIST 800-53, CMS MARS-E] f. The organization shall employ automated mechanisms to facilitate the monitoring and control of remote access methods.	M
AC-17g	g. The information system shall route all remote accesses through a limited number of managed access control points.	M
AC-17h	*[NIST 800-53]* The organization shall: h. Use cryptography to protect the confidentiality and integrity of remote access sessions.	M

Cntl #	Required Control	Risk
AC-17i	i. Authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	M
AC-17j	j. Monitor for unauthorized remote connections to the information system at an organization-defined frequency, and take appropriate action if an unauthorized connection is discovered.	M
AC-17k	k. Ensure that remote sessions for accessing organization-defined list of security functions and security-relevant information employ organization-defined additional security measures and are audited.	M
AC-17l	l. Disable organization-defined networking protocols within the information system deemed to be non-secure except for explicitly identified components in support of specific operational requirements.	M
AC-17m	a. ***[IRS 1075]*** Virtual Private Network (VPN) (or similar technology providing similar protection (e.g., end-to end encryption)) shall be used when remotely accessing the system.	M
AC-18	**1.7.13 AC-18 – Wireless Access [M]** *[NIST 800-53, CMS MARS-E]*	
AC-18	The organization shall prohibit the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization shall:	M
AC-18a	a. Monitor for unauthorized wireless access to the information system.	M
AC-18b	b. Enforce requirements for wireless connections to the information system.	M
AC-18c	c. Protect wireless access to the system using authentication and encryption if wireless access is explicitly approved.	M
AC-18d	[NIST 800-53, IRS 1075] The organization shall d. Establish policy, usage restrictions and implementation guidance for wireless access.	M
AC-18e	e. Authorize wireless access to the information system prior to connection.	M
AC-19	**1.7.14 AC-19 – Access Control for Mobile Devices [M]** *[NIST 800-53, CMS MARS-E]*	
AC-19	The organization shall prohibit the connection of portable and mobile devices [e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations] to information systems **unless explicitly authorized**, in writing, by the CIO or his/her designated representative. **If authorized, the organization shall:**	M
AC-19a	a. Monitor for unauthorized connections of mobile devices to information systems.	M
AC-19b	b. Enforce requirements for the connection of mobile devices to information systems.	M
AC-19c	c. Disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.	M
AC-19d	d. Issue specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	M

Cntl #	Required Control	Risk
AC-19e	*[NIST 800-53, ISO 27001:2005, IRS 1075]* e. The organization shall establish a formal policy, usage restrictions and implementation guidance for organization-controlled mobile devices.	M
AC-19f	*[NIST 800-53]* The organization shall f. Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems.	M
AC-19g	g. Apply organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	M
AC-19h	h. Restrict the use of writable, removable media in organizational information systems.	M
AC-19i	i. Prohibit the use of personally owned, removable media in organizational information systems.	M
AC-19j	j. Prohibit the use of removable media in organizational information systems when the media has no identifiable owner.	M
AC-19k	*[CMS MARS-E]* The organization shall k. Employ an approved method of cryptography to protect information residing on portable and mobile information devices, and utilize whole-disk encryption solution for laptops.	M
AC-19l	l. Protect the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.	M
AC-20	**1.7.15 AC-20 – Use of External Info. Systems [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AC-20	The organization shall prohibit the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information (such as Privacy Act protected information), unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization shall establish strict terms and conditions for their use. The terms and conditions shall address, at a minimum:	M
AC-20a	a. The types of applications that can be accessed from external information systems.	M
AC-20b	**b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted.**	M
AC-20c	c. How other users of the external information system will be prevented from accessing federal information.	M
AC-20d	d. The use of virtual private networking (VPN) and firewall technologies.	M
AC-20e	e. The use of and protection against the vulnerabilities of **wireless** technologies.	M
AC-20f	f. The maintenance of adequate physical security controls.	M
AC-20g	g. The use of virus and spyware protection software.	M
AC-20h	h. How often the security capabilities of installed software are to be updated.	M

Cntl #	Required Control	Risk
AC-20.1a	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or	M
AC-20.1b	b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system	M
AC-20.2	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	M
AC-22	**1.7.16 AC-22 – Publicly Accessible Content [M]** *[NIST 800-53, CMS MARS-E]*	
AC-22a	The organization shall: a. Designate individuals authorized to post information onto an organizational information system that is publicly accessible.	M
AC-22b	b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	M
AC-22c	c. Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.	M
AC-22d	d. Review the content on the publicly accessible organizational information system for nonpublic information at an organization-defined frequency.	M
AC-22e	e. Remove nonpublic information from the publicly accessible organizational information system, if discovered.	M
AU-00	***1.8 Audit and Accountability (AU) Family***	
AU-01	**1.8.1 AU-1 – Audit and Accountability P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AU-01	The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days:	L
AU-01a	a. A formal, documented audit and accountability **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
AU-01b	b. Formal, documented **procedures** to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	L
AU-02	**1.8.2 AU-2 – Auditable Events [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
AU-02a	The organization shall: a. Determine, based on a risk assessment and mission/business needs, that **the information system must be capable of auditing** the following list of auditable events:	M
AU-02a1	i. Server alerts and error messages.	M
AU-02a2	ii. User log-on and log-off (successful or unsuccessful).	M
AU-02a3	iii. All system administration activities.	M

Cntl #	Required Control	Risk
AU-02a4	iv. Modification of privileges and access.	M
AU-02a5	v. Start up and shut down.	M
AU-02a6	vi. Application modifications.	M
AU-02a7	vii. Application alerts and error messages.	M
	viii. Configuration changes.	M
AU-02a9	ix. Account creation, modification, or deletion.	M
AU-02a10	x. File creation and deletion.	M
AU-02a11	xi. Read access to sensitive information.	M
AU-02a12	xii. Modification to sensitive information.	M
AU-02a13	xiii. Printing sensitive information.	M
AU-02b	b. **Coordinate the security audit function with other organizational entities** requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.	M
AU-02c	c. Determine based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.	M
AU-02d	d. Include execution of privileged functions in the list of events to be audited by the information system, including administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors, and access authorizations.	M
AU-02d1	See above.	M
AU-02d2	See above.	M
AU-02d3	See above.	M
AU-02d4	See above.	M
AU-02d5	See above.	M
AU-02d6	See above.	M
AU-02d7	See above.	M
AU-02d8	See above.	M
AU-02e	e. *[NIST 800-53]* The organization shall: Provide a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.	M
AU-02f	f. Review and update the list of auditable events at an organization-defined frequency.	M
AU-03	**1.8.3 AU-3 – Content of Audit Records [M]** *[NIST 800-53, ISO 27001:2005, The Patient Protection and Affordable Care Act, CMS MARS-E, SSA System Security Guidelines]*	
AU-03a	a. The information system shall produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	M
AU-03b	b. The information system shall include the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.	M
AU-04	**1.8.4 AU-4 – Audit Storage Capacity [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AU-04a	a. The organization shall allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.	M

Cntl #	Required Control	Risk
AU-05	**1.8.5 AU-5 – Response to Audit Failures [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AU-05a	The information system shall: a. Alert designated organizational officials in the event of an audit processing failure.	M
AU-05b	b. Take the following additional actions in response to an audit failure or audit storage capacity issue: i. Shutdown the information system. ii. Stop generating audit records. iii. Overwrite the oldest records, in the case that storage media is unavailable.	M
AU-06	**1.8.6 AU-6 – Audit Review, Analysis, Reporting [M]** *[NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*	
AU-06a	The organization shall: a. Review and analyze information system audit records regularly for indications of inappropriate or unusual activity, and report findings to designated organizational officials.	M
AU-06b	b. Adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	M
AU-06.1	**The information system** integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	M
AU-07	**1.8.7 AU-7 – Audit Reduction and Report Generation [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AU-07a	a. The information system shall provide an audit reduction and report generation capability.	M
AU-07b	b. The information system shall provide the capability to automatically process audit records for events of interest based on selectable event criteria.	M
AU-08	**1.8.8 AU-8 – Time Stamps [M]** *[NIST 800-53, CMS MARS-E, IRS 1075, SSA System Security Guidelines]*	
AU-08a	a. The information system shall use internal system clocks to generate time stamps for audit records.	M
AU-08b	b. The information system shall synchronize internal information system clocks daily and at system boot.	M
AU-09	**1.8.9 AU-9 – Protection of Audit Information [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075, SSA System Security Guidelines]*	
AU-09a	a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.	M
AU-10	**1.8.10 AU-10 – Non-Repudiation [M]** *[NIST 800-53, CMS MARS-E]*	
AU-10a	a. The information system shall protect against an individual falsely denying having performed a particular action.	M

Cntl #	Required Control	Risk
AU-11	**1.8.11 AU-11 – Audit Record Retention [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
AU-11a	a. The organization shall retain audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and information retention requirements.	M
AU-11b	[IRS 1075] b. Inspection reports, including a record of corrective actions, shall be retained by the agency for a minimum of three years from the date the inspection was completed. IRS personnel may review these reports during an on-site Safeguard Review.	M
AU-11c	c. To support the audit of activities, all agencies shall ensure that audit information is archived for six years to enable the recreation of computer related accesses to both the operating system and to the application.	M
AU-11d	[SSA System Security Guidelines] d. Each query transaction shall be stored in the audit file as a separate record, not overlaid by subsequent query transactions.	M
AU-11e	e. Audit file data shall be unalterable (read only) and maintained for a minimum of three (preferably seven) years.	M
AU-12	**1.8.12 AU-12 – Audit Generation [M]** *[NIST 800-53, The Patient Protection and Affordable Care Act, CMS MARS-E, HITECH]*	
AU-12a1	The information system shall: a. Provide audit record generation capability for the following events in addition to those specified in other controls: i. All successful and unsuccessful authorization attempts.	M
AU-12a2	ii. All changes to logical access control authorities (e.g., rights, permissions).	M
AU-12a3	iii. All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.	M
AU-12a4	iv. The audit trail shall capture the enabling or disabling of audit report generation services.	M
AU-12a5	v. The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).	M
AU-12b	b. Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system.	M
AU-12c	c. Generate audit records for the list of audited events.	M
AU-12d	d. *[CMS MARS-E]* The information system shall compile audit records from multiple components throughout the system into a system-wide (logical or physical) time-correlated audit trail.	M
AU-12e	e. *[SSA Sys. Sec. Guidelines]* Organizations that receive information electronically from SSA shall be required to maintain an automated audit trail record identifying either the individual user, or the system process, that initiated a request for information from SSA.	M
AU-99	This is a blank formatting row.	
SC-00	***1.9 System and Communications Protection (SC) Family***	

Cntl #	Required Control	Risk
SC-01	**1.9.1 SC-1 – System and Communications Protection P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
SC-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
SC-01a	a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
SC-01b	b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	L
SC-01c	c. *[ISO 27001:2005]* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	L
SC-02	**1.9.2 SC-2 – Application Partitioning [M]** *[NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]*	
SC-02a	a. The information system shall separate user functionality (including user interface services [e.g., web services]) from information system management (e.g., database management systems) functionality.	M
SC-04	**1.9.3 SC-4 – Information in Shared Resources [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SC-04a	a. The information system shall prevent unauthorized and unintended information transfer via shared system resources.	M
SC-05	**1.9.4 SC-5 – Denial of Service Protection [M]** *[NIST 800-53, CMS MARS-E]*	
SC-05a	a. The information system shall protect against or limit the effects of the following types of denial of service attacks defined on the following sites or in the following documents: i. SANS Organization www.sans.org/dosstep. ii. SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php. iii. NIST CVE List http://checklists.nist.gov/home.cfm.	M
SC-05b	b. The information system shall restrict the ability of users to launch denial of service attacks against other information systems or networks.	M
SC-05c	c. The information system shall manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	M
SC-07	**1.9.5 SC-7 – Boundary Protection [M]** *[NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]*	
SC-07a	The information system shall: a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.	M
SC-07b	b. Connect to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with organizational security architecture.	M
SC-07c	c. Physically allocate publicly accessible information system components to separate sub-networks with separate physical network interfaces.	M

Cntl #	Required Control	Risk
SC-07d	d. Prevent public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	M
SC-07e	e. Limit the number of access points to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.	M
SC-07f	f. Ensure the following: i. Implement a managed interface for each external telecommunication service. ii. Establish a traffic flow policy for each managed interface. iii. Employ security controls as needed to protect the confidentiality and integrity of the information being transmitted. iv. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need. v. Review exceptions to the traffic flow policy within every three hundred sixty-five (365) days. vi. Remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need. vii. The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). viii. The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	M
SC-08	**1.9.6 SC-8 – Transmission Integrity [M]** *[NIST 800-53, ISO 27001:2005, The Patient Protection and Affordable Care Act, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
SC-08a	a. The information system shall protect the integrity of transmitted information.	M
SC-08b	b. The organization shall employ cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	M
SC-01	**1.9.7 SC-9 – Transmission Confidentiality [M]** *[NIST 800-53, ISO 27001:2005, The Patient Protection and Affordable Care Act, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075, SSA System Security Guidelines]*	
SC-09a	a. The information system shall protect the confidentiality of transmitted information.	M
SC-09b	b. The organization shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	M
SC-10	**1.9.8 SC-10 – Network Disconnect [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
SC-10a	The information system shall automatically terminate the network connection associated with a communications session at the end of the session, or: a. Forcibly de-allocate communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days.	M
SC-10b	b. Forcibly disconnect inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity.	M
SC-12	**1.9.9 SC-12 – Cryptographic Key Establishment and Management [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	

Cntl #	Required Control	Risk
SC-12a	a. When cryptography is required and used within the information system, the organization shall establish and **manage cryptographic keys** for required cryptography employed within the information system.	M
SC-12b	b. *[IRS 1075]* The organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	M
SC-13	**1.9.10 SC-13 – Use of Cryptography [M]** *[NIST 800-53, ISO 27001:2005, The Patient Protection and Affordable Care Act, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]*	
SC-13a	a. When cryptographic mechanisms are used, the information system shall implement required cryptographic protections using cryptographic modules that comply with applicable federal standards, and guidance.	M
SC-13b	b. When cryptographic mechanisms are used, the organization shall employ, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.	M
SC-13c	c. ***[IRS 1075]*** All Internet transmissions shall be encrypted using HTTPS protocol utilizing Secure Sockets Layer (SSL) encryption based on a certificate containing a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger.	M
SC-13d	[SSA System Security Guidelines] d. The recommended encryption method to secure data in transport for use by SSA shall be the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.	M
SC-14	**1.9.11 SC-14 – Public Access Protections [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
SC-14a	a. The information system shall protect the integrity and availability of publicly available information and applications.	M
SC-15	**1.9.12 SC-15 – Collaborative Computing Devices [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SC-15a	a. The organization shall prohibit running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system shall: i. Prohibit remote activation of collaborative computing devices. ii. Provide an explicit indication of use to users physically present at the devices.	M
SC-15b	b. If collaborative computing is authorized, the information system shall provide physical disconnect of collaborative computing devices in a manner that supports ease of use.	M
SC-17	**1.9.13 SC-17 – Public Key Infrastructure Certs [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
SC-17a	a. When cryptographic mechanisms are used, the information system shall implement required cryptographic protections using cryptographic modules that comply with applicable federal standards, and guidance.	M
SC-17b	b. *[IRS 1075]* The agency shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	M

Cntl #	Required Control	Risk
SC-18	**1.9.14 SC-18 – Mobile Code [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
SC-18a	The organization shall: a. Define acceptable and unacceptable mobile code and mobile code technologies.	M
SC-18b	b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.	M
SC-18c	c. Authorize, monitor, and control the use of mobile code within the information system.	M
SC-19	**1.9.15 SC-19 – Voice Over Internet Protocol [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SC-19a	The organization shall prohibit 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 shall: a. Establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously.	M
SC-19b	b. Authorize, monitor, and control the use of VoIP within the information system.	M
SC-20	**1.9.16 SC-20 – Secure Name Resouce Svc. (Auth Source) [M]** *[NIST 800-53, CMS MARS-E]*	
SC-20a	a. The information system shall provide additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.	M
SC-20b	b. The information system, when operating as part of a distributed, hierarchical namespace, shall provide the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	M
SC-22	**1.9.17 SC-22 – Architecture for Name Res. Svc. [M]** *[NIST 800-53, CMS MARS-E]*	
SC-22a	a. The information systems that collectively provide name/address resolution service for an organization shall be fault tolerant and implement internal/external role separation.	M
SC-23	**1.9.18 SC-23 – Session Authenticity [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SC-23a	a. The information system shall provide mechanisms to protect the authenticity of communications sessions.	M
SC-28	**1.9.19 SC-28 – Protection of Information at Rest [M]** *[NIST 800-53, CMS MARS-E]*	
SC-28a	a. The information system shall protect the confidentiality and integrity of information at rest.	M
SC-32	**1.9.20 SC-32 – Information System Partitioning [M]** *[NIST 800-53, Medicaid Information Tech Architecture, CMS MARS-E]*	

Cntl #	Required Control	Risk
SC-32a	a. The organization shall partition the information system into components residing in separate physical domains (or environments) as deemed necessary.	M
SC-66	**1.9.21 SC-ACA-1 – Electronic Mail [M]-1 – Electronic Mail [M]**	
SC-66a	Controls shall be implemented to protect ACA sensitive information (such as FTI or Privacy Act protected information) that is sent via email. Implementation Standard(s) Prior to sending an email, place all ACA sensitive information in an encrypted attachment. Guidance: A good place to obtain recommended security practices for handling sensitive information via e-mail is NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security. Applicability: All Reference(s): ASSESSMENT PROCEDURE: SC-ACA-1.1 Assessment Objective Determine if: (i) The organization effectively implements protections for ACA sensitive information that is sent via e-mail; (ii) The organization meets all the requirements specified in the applicable implementation standard(s). Examine: Email policy and procedures; other relevant documents or records.	M
SC-99	This is a blank formatting line	
PS-00	***1.10 Personnel Security (PS) Family***	
PS-01	**1.10.1 PS-1 – Personnel Security P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
PS-01	The organization shall develop, disseminate, and review/update within every three hundred sixty-five (365) days:	L
PS-01a	a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
PS-01b	b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	L
PS-01c	[45 CFR Part 160, 162, 164, HIPAA] Policies and procedures shall be implemented: c. For the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	L
PS-01d	d. To determine that the access of a workforce member to electronic protected health information is appropriate.	L
PS-02	**1.10.2 PS-2 – Position Categorization [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
PS-02a	The organization shall: a. Assign a criticality/sensitivity risk designation to all positions.	L
PS-02b	b. Establish screening criteria for individuals filling those positions.	L
PS-02c	c. Review and revise position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.	L
PS-03	**1.10.3 PS-3 – Personnel Screening [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PS-03a	a. The organization shall: Screen individuals prior to authorizing access to the information system.	M
PS-03b	b. Rescreen individuals periodically, consistent with the criticality/sensitivity rating of the position.	M
PS-04	**1.10.4 PS-4 – Personnel Termination [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	

Cntl #	Required Control	Risk
PS-04a	The organization, upon termination of individual employment shall: a. Revoke system and physical access immediately following employee termination.	M
PS-04b	b. Conduct exit interviews.	M
PS-04c	c. Retrieve all security-related information system-related property.	M
PS-04d	d. Retain access to information and information systems formerly controlled by terminated individual.	M
PS-04e	e. Immediately escort employees terminated for cause out of the organization.	M
PS-04f	*[ISO 27001:2005]* f. Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	M
PS-05	**1.10.5 PS-5 – Personnel Transfer [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
PS-05a	The organization shall review logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiate the following transfer or reassignment actions during the formal transfer process: a. Re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes).	M
PS-05b	b. Notification to security management.	M
PS-05c	c. Closing obsolete accounts and establishing new accounts.	M
PS-05d	d. Revocation of all system access privileges (if applicable).	M
PS-06	**1.10.6 PS-6 – Access Agreements [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PS-06a	The organization shall: a. Ensure that individuals requiring access to information or information systems sign appropriate access agreements prior to being granted access.	M
PS-06b	b. Review/update the access agreements as part of the system security authorization or when a contract is renewed or extended.	M
PS-07	**1.10.7 PS-7 – Third-Party Personnel Security [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PS-07a	The organization shall: a. Establish personnel security requirements including security roles and responsibilities for third-party providers.	M
PS-07b	b. Document personnel security requirements.	M
PS-07c	c. Monitor provider compliance.	M
PS-08	**1.10.8 PS-8 – Personnel Sanctions [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075, SSA System Security Guidelines]*	
PS-08a	a. The organization shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.	M
PS-99	This line is a blank formatting line.	
PE-00	***1.11 Physical and Environmental Protection (PE) Family***	

Cntl #	Required Control	Risk
PE-01	**1.11.1 PE-1 – Physical and Envir. Protection P&P [M]** *[NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*	
PE-01	The organization shall develop, disseminate, and review/update within every three hundred sixty-five (365) days:	L
PE-01a	a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
PE-01b	b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	L
PE-02	**1.11.2 PE-2 – Physical Access Authorizations [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
PE-02a	The organization shall: a. Develop and keep current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).	M
PE-02b	b. Issue authorization credentials.	M
PE-02c	c. Review and approve the access list and authorization credentials at least once every one hundred eighty (180) days, removing from the access list personnel no longer requiring access.	M
PE-03	**1.11.3 PE-3 – Physical Access Control [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
PE-03a	The organization shall: a. Enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible).	M
PE-03b	b. Verify individual access authorizations before granting access to the facility.	M
PE-03c	c. Control entry to the facility containing the information system using physical access devices and/or guards.	M
PE-03d	d. Control access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.	M
PE-03e	e. Secure keys, combinations, and other physical access devices.	M
PE-03f	f. Inventory physical access devices within every three hundred sixty-five (365) days.	M
PE-03g	g. Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.	M
PE-03h	h. *[ISO 27001:2005]* Physical protection and guidelines for working in secure areas shall be designed and applied.	M
PE-03i	i. ***[IRS 1075]*** Restricted areas shall be prominently posted and separated from non-restricted areas by physical barriers that control access. The number of entrances shall be kept to a minimum and shall have controlled access (electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance shall be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personnel with an official need enter.	M

Cntl #	Required Control	Risk
PE-03j	j. The agency shall issue authorization credentials to include badges, identification cards and/or smart cards.	M
PE-04	**1.11.4 PE-4 – Access Control for Transmission Medium [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
PE-04a	a. The organization shall control physical access to information system distribution and transmission lines within organizational facilities.	M
PE-04b	*[IRS 1075]* b. Additional precautions shall be taken to protect the cable, (e.g., burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms, and switching centers).	M
PE-04c	c. In instances where encryption is not used, the agency shall ensure that all wiring, conduits, and cabling are within the control of agency personnel and that access to routers and network monitors are strictly controlled.	M
PE-05	**1.11.5 PE-5 – Access Control for Output Devices [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
PE-05a	a. The organization shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	M
PE-06	**1.11.6 PE-6 – Monitoring Physical Access [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PE-06a	The organization shall: a. Monitor physical access to the information system to detect and respond to physical security incidents.	M
PE-06b	b. Review physical access logs at least semi-annually.	M
PE-06c	c. Coordinate results of reviews and investigations with the organization's incident response capability.	M
PE-06d	d. Monitor real-time physical intrusion alarms and surveillance equipment.	M
PE-07	**1.11.7 PE-7 – Visitor Control [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
PE-07a	The organization shall: a. Control physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	M
PE-07b	b. Escort visitors and monitor visitor activity, when required.	M
PE-08	**1.11.8 PE-8 – Access Records [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PE-08a	The organization shall: a. Maintain visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).	M
PE-08b	b. Review visitor access records monthly.	M
PE-08c	c. ***[IRS 1075]*** When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure.	M

Cntl #	Required Control	Risk
PE-08d	d. It is recommended that a second level of management review the register. Each review shall determine the need for access for each individual. To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but are not assigned to the area, an Authorized Access List (AAL) shall be maintained. Each month a new AAL shall be posted at the front desk and vendors shall be required to sign and the monitor shall not be required to make an entry in the restricted area visitor log.	M
PE-08e	e. Designated officials or designees within the organization shall review the visitor access records, at least annually.	M
PE-08f	f. The visitor access log shall contain the following information: i. Name and organization of the visitor ii. Signature of the visitor iii. Form of identification iv. Date of access v. Time of entry and departure vi. Purpose of visit vii. Name and organization of person visited	M
PE-09	**1.11.9 PE-9 – Power Equipment and Cabling [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
PE-09a	a. The organization shall protect power equipment and power cabling for the information system from damage and destruction.	M
PE-10	**1.11.10 PE-10 – Emergency Shutoff [M]** *[NIST 800-53, CMS MARS-E]*	
PE-10a	The organization shall: a. Provide the capability of shutting off power to the information system or individual system components in emergency situations.	M
PE-10b	b. Place emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel.	M
PE-10c	c. Protect emergency power shutoff capability from unauthorized activation.	M
PE-11	**1.11.11 PE-11 – Emergency Power [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
PE-11a	a. The organization shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	M
PE-12	**1.11.12 PE-12 – Emergency Lighting [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
PE-12a	a. The organization shall employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	M
PE-13	**1.11.13 PE-13 – Fire Protection [M]** [NIST 800-53, ISO 27001:2005, CMS MARS-E]	
PE-13a	The organization shall: a. Employ and maintain fire suppression and detection devices/systems for the information system.	M
PE-13b	b. Employ fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.	M

Cntl #	Required Control	Risk
PE-13c	c. Employ fire suppression devices/systems for the information system that provide automatic notification of activation to the organization and emergency responders.	M
PE-13d	d. Employ automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	M
PE-14	**1.11.14 PE-14 – Temp. and Humidity Controls [M]** *[NIST 800-53, CMS MARS-E]*	
PE-14a	The organization shall: a. Maintain temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels.	M
PE-14b	b. Monitor temperature and humidity levels.	M
PE-15	**1.11.15 PE-15 – Water Damage Protection [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
PE-15a	a. The organization shall protect the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	M
PE-16	**1.11.16 PE-16 – Delivery and Removal [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
PE-16a	a. The organization shall authorize, monitor, and control the flow of information system-related components entering and exiting the facility and maintain records of those items.	M
PE-17	**1.11.17 PE-17 – Alternate Work Site [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
PE-17a	The organization shall: a. Employ appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems.	M
PE-17b	b. Assess as feasible, the effectiveness of security controls at alternate work sites.	M
PE-17c	c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.	M
PE-18	**1.11.18 PE-18 – Location of System Components [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
PE-18a	a. The organization shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	
PE-99	This is a blank formatting row.	
CP-00	***1.12 Contingency Planning (CP) Family***	

Cntl #	Required Control	Risk
CP-01	**1.12.1 CP-1 – Contingency Planning P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
CP-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
CP-01a	a. A formal, documented contingency planning **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
CP-01b	b. Formal, documented **procedures** to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	L
CP-02	**1.12.2 CP-2 – Contingency Plan [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]*	
CP-02a	The organization shall: a. Develop a Contingency Plan (CP) for the information system that: i. Identifies essential system missions and business functions and associated contingency requirements. ii. Provides recovery objectives, restoration priorities, and metrics. iii. Addresses contingency roles, responsibilities, assigned individuals with contact information. iv. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure. v. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented. vi. Is reviewed and approved by designated officials within the organization.	M
CP-02b	b. Distribute copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements.	M
CP-02c	c. Coordinate contingency planning activities with incident handling activities.	M
CP-02d	d. Review the CP for the information system within every three-hundred-sixty-five (365) days.	M
CP-02e	e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and	M
CP-02f	f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements.	M
CP-02.1	How does the organization coordinate contingency plan development with organizational elements responsible for related plans?	M
CP-02.2	Describe how and how often the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations and who is responsible for this control implementation.	M
CP-03	**1.12.3 CP-3 – Contingency Training [M]** *[NIST 800-53, CMS MARS-E]*	
CP-03a	a. The organization shall train operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.	M

Cntl #	Required Control	Risk
CP-04	**1.12.4 CP-4 – Contingency Testing and Exercises [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
CP-04a	a. (i) Contingency Plans shall be tested and/or exercised at least every 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS Procedures, to determine the plans' effectiveness and readiness to execute the plan. (ii) Test / exercise results shall be documented and reviewed by appropriate organization officials. (iii) Reasonable and appropriate corrective actions shall be initiated to close or reduce the impact of Contingency Plan failures and deficiencies.	M
CP-06	**1.12.5 CP-6 – Alternate Storage Site [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CP-06a	The organization shall: a. Establish an alternate storage site including necessary agreements to permit the storage and recovery of system backup information.	M
CP-06b	b. Identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	M
CP-06c	c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	M
CP-07	**1.12.6 CP-7 – Alternate Processing Site [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CP-07a	The organization shall: a. Establish an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within one (1) week when the primary processing capabilities are unavailable.	M
CP-07b	b. Ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site within one (1) week.	M
CP-07c	c. Identify an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	M
CP-07d	d. Identify potential accessibility problems to the alternate processing site in the event of an area wide disruption or disaster and outline explicit mitigation actions.	M
CP-07e	e. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	M
CP-07f	f. Ensure that the alternate processing site provides information security measures equivalent to that of the primary site.	M
CP-08	**1.12.7 CP-8 – Telecommunications Services [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CP-08a	The organization shall: a. Establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when the primary telecommunications capabilities are unavailable.	M

Cntl #	Required Control	Risk
CP-08b	b. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	M
CP-08c	c. Request Telecommunications Service Priority for telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	M
CP-08d	d. Obtain alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	M
CP-09	**1.12.8 CP-9 – Information System Backup [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
CP-09a	The organization shall: a. Conduct weekly backups of user-level information contained in the information system.	M
CP-09b	b. Conduct weekly backups of system-level information contained in the information system.	M
CP-09c	c. Conduct backups of information system documentation including security-related documentation and other forms of data, including paper records.	M
CP-09d	d. Protect the confidentiality and integrity of system backup information at the storage location.	M
CP-09e	e. Test backup information following each backup to verify media reliability and information integrity.	M
CP-09f	f. *[IRS 1075]* On line data resources shall be provided adequate tools for the back-up, storage, restoration, and validation of data. Both incremental and special purpose data back-up procedures shall be required, combined with off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity.	M
CP-10	**1.12.9 CP-10 – Information System Recovery [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]*	
CP-10a	a. The organization shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.	M
CP-10b	b. The information system shall implement transaction recovery for systems that are transaction-based.	M
CP-10c	c. The organization shall provide Compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.	M
CP-99	This is a blank formatting line.	
CM-00	***1.13 Configuration Management (CM)***	
CM-01	**1.13.1 CM-1 – Configuration Management P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
CM-01	The organization shall develop, disseminate, and review/update within every three-hundred sixty-five (365) days:	L

Cntl #	Required Control	Risk
CM-01a	a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
CM-01b	b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	L
CM-02	**1.13.2 CM-2 – Baseline Configuration [M]** *[NIST 80-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
CM-02a	The organization shall: a. Develop, document, and maintain under configuration control, a current baseline configuration of the information system.	M
CM-02b	b. Review and update the baseline configuration of the information system: i. At least once every three-hundred-sixty-five (365) days. ii. When required due to major system changes/upgrades. iii. As an integral part of information system component installations and upgrades.	M
CM-02c	c. Retain older versions of baseline configurations as deemed necessary to support rollback.	M
CM-02d	d. Develop and maintain a list of software programs authorized (white list) or unauthorized (black list) to execute on the information system.	M
CM-02e	e. Employ an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.	M
CM-03	**1.13.3 CM-3 – Configuration Change Control [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
CM-03a	The organization shall: a. Determine the types of changes to the information system that are configuration controlled.	M
CM-03b	b. Approve configuration-controlled changes to the system with explicit consideration for security impact analyses.	M
CM-03c	c. Document approved configuration-controlled changes to the system.	M
CM-03d	d. Retain and review records of configuration-controlled changes to the system.	M
CM-03e	e. Audit activities associated with configuration-controlled changes to the system.	M
CM-03f	f. Coordinate and provide oversight for configuration change control activities through change request forms that must be approved by an organizational and/or change control board that meets frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.	M
CM-03g	g. Test, validate, and document changes to the information system before implementing the changes on the operational system.	M
CM-04	**1.13.4 CM-4 – Security Impact Analysis [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
CM-04a	The organization shall a. Analyze changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system shall be audited.	M

Cntl #	Required Control	Risk
CM-04b	b. Analyze new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	M
CM-04c	c. After the information system is changed, check the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.	M
CM-04.1	The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	M
CM-05	**1.13.5 CM-5 – Access Restrictions for Change [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CM-05a	a. The organization shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	M
CM-05a2	Continued from above.	
CM-06	**1.13.6 CM-6 – Configuration Settings [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
CM-06a	The organization shall: a. Establish and document mandatory configuration settings for information technology products employed within the information system using the latest security configuration baselines established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 that reflect the most restrictive mode consistent with operational requirements. i. HHS-specific minimum security configurations shall be used for the following Operating System (OS) and Applications: • HHS FDCC Windows XP Standard • HHS FDCC Windows Vista Standard • Blackberry Server • Websense ii. For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is as follows: • USGCB • NIST National Checklist Program (NCP); Tier IV, then Tier III, Tier II, and Tier I, in descending order. • Defense Information Systems Agency (DISA) STIGs • National Security Agency (NSA) STIGs • If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists. • In situations where no guidance exists, coordinate with CMS for guidance. CMS shall collaborate within CMS and the HHS Cyber security Program, and other OPDIVs through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to establish baselines and communicate industry and vendor leading practices. • All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented in an approved HHS waiver (available at http://intranet.hhs.gov/it/cybersecurity/policies_by_document_type/index.html#Policy and Standard Waiver), with copies submitted to the Department.	M
CM-06b	b. Implement the configuration settings.	M
CM-06c	c. Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements.	M
CM-06d	d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	M
CM-06e	e. Incorporate detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	M
CM-07	**1.13.7 CM-7 – Least Functionality [M]** *[NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]*	

Cntl #	Required Control	Risk
CM-07a	The organization shall: a. Configure the information system to provide only essential capabilities and specifically disable, prohibit, or restrict the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols shall be maintained and documented in the SSP; all others shall be disabled.	M
CM-07b	b. Review the information system within every three-hundred-sixty-five (365) days to identify and eliminate unnecessary functions, ports, protocols, and/or services.	M
CM-08	**1.13.8 CM-8 – System Component Inventory [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
CM-08a	a. The organization shall develop, document, and maintain an inventory of information system components that: i. Accurately reflects the current information system. ii. Is consistent with the authorization boundary of the information system. iii. Is at the level of granularity deemed necessary for tracking and reporting. iv. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership. v. Is available for review and audit by designated organizational officials.	M
CM-08b	b. The organization shall update the inventory of information system components as an integral part of component installations, removals, and information system updates.	M
CM-08c	c. The organization shall verify that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	M
CM-09	**1.13.9 CM-9 – Configuration Management Plan [M]** *[NIST 800-53, CMS MARS-E]*	
CM-09a	The organization shall develop, document, and implement a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures.	M
CM-09b	b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management.	M
CM-09c	c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	M
CM-99	Blank formatting line.	
MA-00	***1.14 Maintenance (MA) Family***	
MA-01	**1.14.1 MA-1 – System Maintenance P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
MA-01	The organization shall develop, disseminate, and review/update within every three hundred sixty-five (365) days:	L

Cntl #	Required Control	Risk
MA-01a	a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
MA-01b	b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	L
MA-02	**1.14.2 MA-2 – Controlled Maintenance [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
MA-02a	The organization shall: a. Schedule, perform, document, and review records of maintenance and repair on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	M
MA-02b	b. Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.	M
MA-02c	c. Require that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	M
MA-02d	d. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.	M
MA-02e	e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	M
MA-02f	f. Maintain maintenance records for the information system that include: i. Date and time of maintenance. ii. Name of the individual performing the maintenance. iii. Name of escort, if necessary. iv. A description of the maintenance performed. v. A list of equipment removed or replaced (including identification numbers, if applicable).	M
MA-03	**1.14.3 MA-3 – Maintenance Tools [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
MA-03a	The organization shall: a. Approve, control, monitor the use of, and maintain on an ongoing basis, information system maintenance tools.	M
MA-03b	b. Inspect all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.	M
MA-03c	c. Check all media containing diagnostic and test programs for malicious code before the media is used in the information system.	M
MA-04	**1.14.4 MA-4 – Non-Local Maintenance [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
MA-04	The organization **shall prohibit non-local system maintenance unless explicitly authorized, in writing, by the CIO** or his/her designated representative. If authorized, the organization shall:	M
MA-04a	a. **Monitor** and control non-local maintenance and diagnostic activities. *(CMS clarification: who authorizes and who maintains the authorization document.)*	M
MA-04b	b. Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.	M
MA-04c	c. Employ **strong identification and authentication** techniques in the establishment of non-local maintenance and diagnostic sessions.	M

Cntl #	Required Control	Risk
MA-04d	d. Maintain records for non-local maintenance and diagnostic activities.	M
MA-04e	e. Terminate all sessions and network connections when non-local maintenance is completed.	M
MA-04f	f. ***Not required per CMS – 2014-02-27*** Audit non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.	M
MA-04g	g. ***Not required per CMS – 2014-02-27*** Document, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	M
MA-04h	h. ***Not required per CMS – 2014-02-27*** Require that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced.	M
MA-04i	i. ***NR CMS – 2014-02-27*** Remove the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitize the component (with regard to sensitive information such as Privacy Act protected information) before removal from organizational facilities, and after the service is performed, inspect and sanitize the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.	M
MA-05	**1.14.5 MA-5 – Maintenance Personnel [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
MA-05a	The organization shall: a. Establish a process for **maintenance personnel authorization** and maintain a current list of authorized maintenance organizations or personnel.	M
MA-05b	b. Ensure that personnel performing maintenance on the information system have required access authorizations or designate organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	M
MA-06	**1.14.6 MA-6 – Timely Maintenance [M]** *[NIST 800-53, CMS MARS-E]*	
MA-06a	a. The organization shall obtain maintenance support and/or spare parts for critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within twenty-four (24) hours of failure.	M
MA-99	This is a blank formatting row.	
SI-00	***1.15 System and Information Integrity (SI)***	
SI-01	**1.15.1 SI-1 – System and Info Integrity P&P [M]** *[NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*	
SI-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
SI-01a	a. A formal, documented system and information integrity **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L

Cntl #	Required Control	Risk
SI-01b	b. Formal, documented **procedures** to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	L
SI-02	**1.15.2 SI-2 – Flaw Remediation [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SI-02a	The organization shall: a. Identify, report, and correct information system flaws.	M
SI-02b	b. Test software updates related to flaw remediation for effectiveness and potential side effects on information systems before installation.	M
SI-02c	c. Incorporate flaw remediation into the organizational configuration management process.	M
SI-02d	d. Centrally manage the flaw remediation process and install software updates automatically.	M
SI-02e	e. Employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.	M
SI-03	**1.15.3 SI-3 – Malicious Code Protection [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
SI-03a	The organization shall: a. Employ malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: i. Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means. ii. Inserted through the exploitation of information system vulnerabilities.	M
SI-03b	b. Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures.	M
SI-03c	c. Configure malicious code protection mechanisms to: i. Perform critical system file scans during system boot, information system scans every twenty-four (24) hours, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy. ii. Block and quarantine malicious code and send alert to administrator in response to malicious code detection.	M
SI-03d	d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	M
SI-03e	e. Centrally manage malicious code protection mechanisms.	M
SI-03f	f. Ensure that the information system automatically updates malicious code protection mechanisms (including signature definitions).	M
SI-03g	g. Ensure that the information system prevents non-privileged users from circumventing malicious code protection capabilities.	M
SI-03h	h. *[ISO 27001:2005]* The organization shall implement appropriate user awareness procedures.	M
SI-04	**1.15.4 SI-4 – Information System Monitoring [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	

Cntl #	Required Control	Risk
SI-04a	The organization shall: a. Monitor events on the information system in accordance with Information Security Incident Handling and Breach Analysis/ Notification Procedure and detect system attacks.	M
SI-04b	b. Identify unauthorized use of the system.	M
SI-04c	c. Deploy monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.	M
SI-04d	d. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	M
SI-04e	e. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	M
SI-04f	f. Interconnect and configure individual intrusion detection tools into a system wide intrusion detection system using common protocols.	M
SI-04g	g. Employ automated tools to support near real-time analysis of events.	M
SI-04h	h. Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.	M
SI-04i	i. Ensure that the information system provides near real-time alerts when the following indications of compromise or potential compromise occur: i. Presence of malicious code. ii. Unauthorized export of information. iii. Signaling to an external information system. iv. Potential intrusions.	M
SI-04j	j. Ensure that the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	M
SI-04k	[SSA System Security Guidelines] k. The system shall produce reports providing management and/or supervisors with the capability to appropriately monitor user activity, such as: i. User ID exception reports: This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password. ii. Inquiry match exception reports: This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the organization system. iii. System error exception reports: This type of report captures information about users who may not understand or be following proper procedures for access to SSA information. iv. Inquiry activity statistical reports: This type of report captures information about transaction usage patterns among authorized users, which would provide a tool to the organization's management for monitoring typical usage patterns compared to extraordinary usage.	M
SI-05	**1.15.5 SI-5 – Security Alerts, Advisories, and Directives [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
SI-05a	The organization shall: a. Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.	M

Cntl #	Required Control	Risk
SI-05b	b. Generate internal security alerts, advisories, and directives as deemed necessary.	M
SI-05c	c. Disseminate security alerts, advisories, and directives to appropriate personnel.	M
SI-05d	d. Implement security directives in accordance with established time frames, or notifies the degree of noncompliance.	M
SI-07	**1.15.6 SI-7 – Software and Information Integrity [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]*	
SI-07a	a. The information system shall detect unauthorized changes to software and information.	M
SI-07b	b. The organization shall reassess the integrity of software and information by performing daily integrity scans of the information system.	M
SI-07c	c. *[ISO 27001:2005]* Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	M
SI-08	**1.15.7 SI-8 – Spam Protection [M]** *[NIST 800-53, CMS MARS-E]*	
SI-08a	The organization shall: a. Employ spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.	M
SI-08b	b. Update spam protection mechanisms (including signature definitions) when new releases are available in accordance with configuration management policy and procedures.	M
SI-08c	c. Centrally manage spam protection mechanisms.	M
SI-08.1	SI-8(1) – Enhancement [M] Control The organization centrally manages spam protection mechanisms.	M
SI-09	**1.15.8 SI-9 – Information Input Restrictions [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SI-09a	a. The organization shall restrict the capability to input information to the information system to authorized personnel.	M
SI-10	**1.15.9 SI-10 – Information Input Validation [M]** *[NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E]*	
SI-10a	a. The information system shall use automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.	M
SI-11	**1.15.10 SI-11 – Error Handling [M]** *[NIST 800-53, CMS MARS-E]*	
SI-11a	The information system shall: a. Identify potentially security-relevant error conditions.	M
SI-11b	b. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries.	M

Cntl #	Required Control	Risk
SI-11c	c. Reveal error messages only to authorized personnel.	M
SI-12	**1.15.11 SI-12 – Information Output Handling and Retention [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
SI-12a	a. The organization shall **handle and retain** both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	M
SI-99	This is a blank formatting line	
MP-00	***1.16 Media Protection (MP) Family***	
MP-01	**1.16.1 MP-1 – Media Protection P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*	
MP-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
MP-01a	a. A formal, documented media protection **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
MP-01b	b. Formal, documented **procedures** to facilitate the implementation of the media protection policy and associated media protection controls.	L
MP-01c	*[45 CFR Part 160, 162, 164, HIPAA]* c. Policies and procedures shall be implemented that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	L
MP-02	**1.16.2 MP-2 – Media Access [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
MP-02a	The organization shall a. Restrict access to sensitive (such as Private Act protected) information residing on digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.	M
MP-02b	b. Employ automated mechanisms to audit access attempts and access granted.	M
MP-03	**1.16.3 MP-3 – Media Marking [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
MP-03a	The organization shall: a. Mark, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	M
MP-03b	b. Exempt specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment.	M
MP-04	**1.16.4 MP-4 – Media Storage [M]**	
MP-04a	[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075] The organization shall: a. Physically control and securely store digital and non-digital media within controlled areas using safeguards prescribed for the highest system security level of the information ever recorded on it.	M

Cntl #	Required Control	Risk
MP-04b	b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	M
MP-05	**1.16.5 MP-5 – Media Transport [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
MP-05a	The organization shall: a. Protect and control digital and non-digital media containing sensitive information (such as Privacy Act information) during transport outside of controlled areas using cryptography and tamper evident packaging and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, track able with receipt by commercial carrier.	M
MP-05b	b. Maintain accountability for information system media during transport outside of controlled areas.	M
MP-05c	c. Restrict the activities associated with transport of such media to authorized personnel.	M
MP-05d	d. Document activities associated with the transport of information system media.	M
MP-05e	e. Employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	M
MP-06	**1.16.6 MP-6 – Media Sanitization [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]*	
MP-06a	a. The organization shall: Sanitize information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.	M
MP-06b	b. Employ sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	M
MP-06c	c. *[CMS MARS-E]* The organization shall: i. Track, document, and verify media sanitization and disposal actions. ii. Test sanitization equipment and procedures to verify correct performance periodically. iii. Sanitize information system media containing sensitive information (such as Privacy Act protected information) using National Security Agency (NSA) guidance. iv. Destroy media containing sensitive information (such as Privacy Act protected information) that cannot be sanitized.	M
MP-06.1	Describe how the organization tracks, documents, and verifies media sanitization and disposal actions.	M
MP-06.2	Describe the process/procedure for how the organization tests sanitization equipment and procedures to verify correct performance periodically. (state what the frequency is).	M
MP-06.5	Describe how the organization sanitizes information system media containing sensitive information using National Security Agency (NSA) guidance and NIST SP 800-88, Guidelines for Media Sanitization.	M
MP-06.6	Describe the organization's process for destroying media containing sensitive information that cannot be sanitized.	M
MP-07	**1.16.7 MP-ACA-1 – Media Related Records [M]** *[CMS MARS-E]*	
MP-07a	a. Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.	M

Cntl #	Required Control	Risk
MP-99	This is a blank formatting row.	
IR-00	***1.17 Incident Response (IR) Family***	
IR-01	**1.17.1 IR-1 – Incident Response P&P [M]** *[NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*	
IR-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L
IR-01a	a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L
IR-01b	b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	L
IR-02	**1.17.2 IR-2 – Incident Response Training [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
IR-02a	The organization shall: a. Train personnel in their incident response roles and responsibilities with respect to the information system.	M
IR-02b	b. Provide refresher training within every three-hundred-sixty-five (365) days.	M
IR-03	**1.17.3 IR-3 – Incident Response Exercises [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
IR-03a	a. The organization shall test and/or exercise the incident response capability for the information system annually using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results.	M
IR-04	**1.17.4 IR-4 – Incident Handling [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]*	
IR-04a	The organization shall: a. Implement an incident handling capability using Information Security Incident Handling and Breach Notification Procedures.	M
IR-04b	b. Coordinate incident handling activities with contingency planning activities.	M
IR-04c	c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.	M
IR-04d	d. Employ automated mechanisms to support the incident handling process.	M
IR-04e	e. *[ISO 27001:2005]* There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	M
IR-05	**1.17.5 IR-5 – Incident Monitoring [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
IR-05a	a. The organization tracks and documents information system security incidents.	M
IR-06	**1.17.6 IR-6 – Incident Reporting [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, HIPAA]*	

Cntl #	Required Control	Risk
IR-06a	The organization shall: a. Require personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current Information Security Incident Handling and Breach Analysis/Notification Procedure.	M
IR-06b	b. Report security incident information to designated authorities.	M
IR-06c	c. The organization shall employ automated mechanisms to assist in the reporting of security incidents.	M
IR-06.1	The organization employs automated mechanisms to assist in the reporting of security incidents.	M
IR-07	**1.17.7 IR-7 – Incident Response Assistance [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*	
IR-07a	a. The organization shall: Provide an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	M
IR-07b	b. *[NIST 800-53, CMS MARS-E]* The organization shall employ automated mechanisms to increase the availability of incident response-related information and support.	M
IR-08	**1.17.8 IR-8 – Incident Response Plan [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
IR-08a	The organization shall: a. Develop an incident response plan that: i. Provides the organization with a roadmap for implementing its incident response capability. ii. Describes the structure and organization of the incident response capability. iii. Provides a high-level approach for how the incident response capability fits into the overall organization. iv. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions. v. Defines reportable incidents. vi. Provides metrics for measuring the incident response capability within the organization. vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and viii. Is reviewed and approved by designated officials within the organization.	M
IR-08b	b. Distribute copies of the incident response plan to incident response personnel and organizational elements.	M
IR-08c	c. Review the incident response plan within every three-hundred-sixty-five (365) days.	M
IR-08d	d. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	M
IR-08e	e. Communicate incident response plan changes to incident response personnel and organizational elements.	M
IR-99	This is a blank formatting row.	
AT-00	***1.18 Awareness and Training (AT) Family***	
AT-01	**1.18.1 AT-1 – Security Awareness Training P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	

Cntl #	Required Control	Risk
AT-01	The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:	L
AT-01a	a. A formal, documented security awareness and training **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	L
AT-01b	b. Formal, documented **procedures** to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	L
AT-02	**1.18.2 AT-2 – Security Awareness [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, SSA System Security Guidelines]*	
AT-02a	a. The organization shall provide **basic security awareness training** to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three-hundred sixty-five (365) days thereafter.	M
AT-02b	b. *[IRS 1075]* Agencies shall make employees aware that disclosure restrictions and the penalties apply even after employment with the agency has ended. Security information and requirements shall be expressed to appropriate personnel by using a variety of methods, such as: Formal and informal training.; Discussion at group and managerial meetings.; Install security bulletin boards throughout the work areas.; Place security articles in employee newsletters.; Route pertinent articles that appear in the technical or popular press to members of the management staff.; Display posters with short simple educational messages (e.g., instructions on reporting unauthorized access "UNAX" violations, address, and hotline number).; Use warning banners during initial logon.; Send e-mail and other electronic messages to inform users.	M
AT-02c	c. *[SSA System Security Guidelines]* All persons who will have access to any SSA information shall be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws.	M
AT-02d	d. Security awareness training shall address the Privacy Act and other Federal and State laws governing use and misuse of protected information.	M
AT-02e	e. *[ISO 27001:2005]* The organization shall detect, prevent, and recover controls to protect against malicious code and implement appropriate user awareness procedures.	M
AT-03	**1.18.3 AT-3 – Security Training [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*	
AT-03a	a. The organization shall provide role-based security-related training: i. Before authorizing access to the system or performing assigned duties. ii. When required by system changes. iii. Refresher training within every three hundred sixty-five (365) days thereafter.	M
AT-03a2		M
AT-03b	*[IRS 1075]* b. This training shall cover situations that could occur as the result of an interruption of work by family, friends, or other sources.	M
AT-03c	c. *[SSA System Security Guidelines]* Employees granted access to SSA information shall receive adequate training on the sensitivity of the information, safeguards that shall be followed, and the penalties for misuse, and shall perform periodic self-reviews to monitor ongoing usage of the online access to SSA information.	M

Cntl #	Required Control	Risk
AT-04	**1.18.4 AT-4 – Security Training Records [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*	
AT-04a	The organization shall: a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training.	M
AT-04b	b. Retain individual training records for three (3) years.	M
AT-99	This is a blank formatting line.	
zz-99	☐	

Appendix A – Vendor documentation

Appendix B – Contracts, etc.

Appendix C – Acronyms and Abbreviations

Acronym	Term
AC	Access Control
ACA	Patient Protection and Affordable Care Act of 2010
AD	Microsoft Active Directory
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
APIPA	Automatic Private IP Addressing
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CCB	Change Control Board
CFR	Code of Federal Regulations
CI	Configuration Item
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMS	Centers for Medicare & Medicaid Services
CMRS	Continuous Monitoring and Risk Scoring
CMSR	CMS Minimum Security Requirements
COOP	Continuity of Operations Plan
CP	Contingency Planning
DES	Data Encryption Standard
DHSS	Department of Health and Social Services
DIFSLA	IRS Publication 3373 Disclosure of Information to Federal, State, and Local Agencies
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoS	Denial of Service
DPA	Division of Public Assistance
DR	Disaster Recovery
DSO	Department Security Office
EIS-R	Eligibility Information System – Replacement
EPHI	Electronic protected health information

Acronym	Term
LAN	Local area network
MA	Maintenance
MARS	Minimum Security Controls for Exchanges – Exchange Reference Architecture Supplement
MITA	Medicaid Information Technology Architecture
MP	Media Protection
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
OMB	Office of Management and Budget
PDA	Personal digital assistants
PE	Physical and Environmental Protection
PHI	Protected Health Information
PHR	Personal Health Record
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PL	Planning
PM	Information Security Program Plan
POA	Plan of Action
POA&M	Plan of Action and Milestones
PS	Personnel Security
PUB	Publication
RA	Risk Assessments
RAC-F	Resource Access Control Facility
ROB	Rules of Behavior
RSS	Registration Support Specialist
SA	System and Services Acquisition
SAR	Safeguard Activity Report
SAM	Security Access Manager
SC	System and Communications Protection
SDLC	Software Development Lifecycle

Acronym	Term
ESI	Electronically Stored Information
FIPS	Federal Information Processing Standards
FTI	Federal Tax Information
GSS	General Support Systems
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
HTTPS	Hypertext Transfer Protocol Secure
IA	Identification and Authentication
ID	Identifier
IDS	Intrusion detection system
INR	Incident Response Report
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
IRS	Internal Revenue Service
IRT	Incident Response Team
IS	Information Security
ISO	International Organization for Standardization
IT	Information Technology

Acronym	Term
SFTP	Secure File Transfer Protocol
SI	System and Information Integrity
SOA	State Of Alaska
SSA	Social Security Administration
SSL	Secure Sockets Layer
SSN	Social Security Number
SSO	State Security Office
SSP	System Security Plan
TLS	Transport Layer Security
URL	Uniform Resource Locator
USGCB	U.S. Government Configuration Baselines
VLAN	Virtual Local Area Network
VM	Vulnerability Management
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Points
WP	Worker Portal