For the RFP, the vendor will state at a high-level how the vendor and proposed system will comply with each of the following families of issues.

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

A deliverable for the product will be a completed document (sample provided) showing vendor and system compliance with the NIST SP800-53 requirements.

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
1.	010000	RA-00	***1.1 Risk Assessment (RA) Family***				
2.	010100	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]*				
3.	010101	RA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
4.	010102	RA-01a	a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	I	a.	
5.	010103	RA-01b	b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	L	P	b.	
6.	010200	RA-02	**1.1.2 RA-2 – Security Categorization [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
7.	010201	**RA-02a**	The organization shall: a. Categorize information and the information system in accordance with applicable federal standards and guidance.	M		a.	
8.	010202	**RA-02b**	b. Document the security categorization results (including supporting rationale) in the security plan for the information system.	M		b.	
9.	010203	**RA-02c**	c. Ensure the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	M		c.	
10.	010300	**RA-03**	**1.1.3 RA-3 – Risk Assessment [M]** *[NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]*				
11.	010301	**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		i.	
12.	010302	**RA-03b**	b. Document risk assessment results.	M		a.	
13.	010303	**RA-03c**	c. Review risk assessment results within every three-hundred-sixty-five (365) days.	M		b.	
14.	010304	**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		c.	
15.	010305	**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		d.	
16.	010306	**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		e.	
17.	010400	**RA-05**	**1.1.4 RA-5 – Vulnerability Scanning [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
18.	010401	**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		a.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
19.	010402	**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		i.	
20.	010403	**RA-05c**	c. Analyze vulnerability scan reports and results from security control assessments.	M		b.	
21.	010404	**RA-05d**	d. Remediate legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk.	M		c.	
22.	010405	**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		d.	
23.	010406	**RA-05f**	f. Employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	M		e.	
24.	019900	**RA-99**	This line is a blank spacer line.				
25.	020000	**PL-00**	***1.2 Planning (PL) Family***				
26.	020100	**PL-01**	**1.2.1 PL-1 – Security Planning P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
27.	020101	**PL-01**	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
28.	020102	**PL-01a**	a. A formal, documented security planning **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	I	a.	
29.	020103	**PL-01b**	b. Formal, documented **procedures** to facilitate the implementation of the security planning policy and associated security planning controls.	L	P	b.	
30.	020200	**PL-02**	**1.2.2 PL-2 – System Security Plan (SSP) [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
31.	020201	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 ARIES system. iv. Describes the operational context of the ARIES system in terms of missions and business processes. v. Describes the operational environment for the ARIES system. vi. Describes relationships with or connections to other information systems. vii. Provides an overview of the security requirements for the ARIES 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		i.	
32.	020202	PL-02b	b. Review the security plan for the information system within every three-hundred-sixty-five (365) days.	M		a.	
33.	020203	PL-02c	c. Update the plan, minimally every three (3) years, to address current conditions or whenever: i. There are significant changes to the ARIES 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		i.	
34.	020300	PL-04	**1.2.3 PL-4 – Rules of Behavior (ROB) [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
35.	020301	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		i.	
36.	020302	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		a.	
37.	020303	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		b.	
38.	020400	PL-05	**1.2.4 PL-5 – Privacy Impact Assessment (PIA) [M]** *[NIST 800-53, CMS MARS-E]*				
39.	020401	PL-05a	a. The organization shall conduct a Privacy Impact Assessment (PIA) in accordance with OMB policy M-03-22.	M		a.	
40.	020500	PL-06	**1.2.5 PL-6 – Security-Related Activity Planning [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
41.	020501	**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		a.	
42.	029900	**PL-99**	This is a blank formatting row.				
43.	030000	**SA-00**	***1.3 System and Services Acquisition (SA)***				
44.	030100	**SA-01**	**1.3.1 SA-1 – System& Services Acquisition P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
45.	030101	**SA-01**	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
46.	030102	**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	I	a.	
47.	030103	**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	P	b.	
48.	030200	**SA-02**	**1.3.2 SA-2 – Allocation of Resources [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
49.	030201	**SA-02a**	The organization shall: a. Include a determination of information security requirements for the information system in mission/business process planning.	M		a.	
50.	030202	**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		b.	
51.	030203	**SA-02c**	c. Include information security requirements in mission/business case planning.	M		c.	
52.	030204	**SA-02d**	d. Establish a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.	M		d.	
53.	030300	**SA-03**	**1.3.3 SA-3 – Life Cycle Support [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
54.	030301	**SA-03a**	The organization shall: a. Manage the lifecycle of the information system.	M		a.	
55.	030302	**SA-03b**	b. Define and document information system security roles and responsibilities throughout the system development life cycle.	M			
56.	030303	**SA-03c**	c. Identify individuals having information system security roles and responsibilities.	M			
57.	030400	**SA-04**	**1.3.4 SA-4 – Acquisitions [M]** *[NIST 800-53, CMS MARS-E]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
58.	230401	**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			
59.	230402	**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		a.	
60.	230403	**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		b.	
61.	230404	**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.				
62.	230405	**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.				
63.	230500	**SA-05**	**1.3.5 SA-5 – System Documentation [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
64.	230501	**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		•	
65.	230502	**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		•	
66.	230503	**SA-05c**	c. Document attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	M		a.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
67.	230504	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		i.	
68.	230505	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		b.	
69.	230600	SA-06	**1.3.6 SA-6 – Software Usage Restrictions [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
70.	230601	SA-06a	The organization shall: a. Use software and associated documentation in accordance with contract agreements and copyright laws.	M		a.	
71.	230602	SA-06b	b. Employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.	M		b.	
72.	230603	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		c.	
73.	230700	SA-07	**1.3.7 SA-7 – User-Installed Software [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
74.	230701	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		a.	
75.	230800	SA-08	**1.3.8 SA-8 – Security Engineering Principles [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
76.	230801	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			
77.	230900	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]*				
78.	230901	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			
79.	230902	SA-09b	b. Define and document oversight and user roles and responsibilities with regard to external information system services.	M			

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
80.	230903	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			
81.	230904	SA-09d	d. Monitor security control compliance by external service providers.	M			
82.	230905	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		i.	
83.	230906	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		e.	
84.	230907	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		f.	
85.	231000	SA-10	**1.3.10 SA-10 – Developer Configuration Mgmt [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
86.	231001	SA-10a	The organization shall require that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation.	M		a.	
87.	231002	SA-10b	b. Manage and control changes to the information system.	M		b.	
88.	231003	SA-10c	c. Implement only organization-approved changes.	M		c.	
89.	231004	SA-10d	d. Document approved changes to the information system.	M		d.	
90.	231005	SA-10e	e. Track security flaws and flaw resolution.	M		e.	
91.	231100	SA-11	**1.3.11 SA-11 – Developer Security Testing [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
92.	231101	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		a.	
93.	231102	SA-11b	b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process.	M			
94.	231103	SA-11c	c. Document the results of the security control assessment and flaw remediation processes.	M		i.	
95.	231104	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		b.	
96.	239900	SA-99	This line is a blank spacer line.				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
97.	040000	**CA-00**	***1.4 Security Assessment and Authorization (CA) Family***				
98.	040100	**CA-01**	**1.4.1 CA-1 – Security Assessment and Authorization P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
99.	040101	CA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
100.	040102	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	In	a.	
101.	040103	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	P	b.	
102.	040200	**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]*				
103.	040201	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			
104.	040202	**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		a.	
105.	040203	**CA-02c**	c. Produce a security assessment report that documents the results of the assessment.	M		b.	
106.	040204	**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		c.	
107.	040205	**CA-02e**	e. Employ an independent assessor or assessment team to conduct an assessment of the security controls.	M		d.	
108.	040300	**CA-03**	**1.4.3 CA-3 – Information System Connections [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
109.	040301	**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		a.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
110.	040302	CA-03b	b. Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.	M		b.	
111.	040303	CA-03c	c. Monitor the information system connections on an ongoing basis verifying enforcement of security requirements.	M		c.	
112.	040304	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		d.	
113.	040400	CA-05	**1.4.4 CA-5 – Plan of Action and Milestones [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
114.	040401	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		a.	
115.	040402	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		b.	
116.	040403	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		c.	
117.	040500	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]*				
118.	040501	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		a.	
119.	040502	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		i.	
120.	040600	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]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
121.	040601	**CA-07a**	a. The organization shall establish a continuous monitoring strategy and implement a continuous monitoring program that includes:	M		a.	
122.	040602	**CA-07a1**	i. A configuration management process for the information system and its constituent components.	M		i.	
123.	040603	**CA-07a2**	ii. A determination of the security impact of changes to the information system and environment of operation.	M		ii.	
124.	040604	**CA-07a3**	iii. Ongoing security control assessments in accordance with **the organizational continuous monitoring strategy.**	M		iii.	
125.	040605	**CA-07a4**	iv. Reporting the security state of the information system to appropriate organizational officials within every three-hundred-sixty-five (365) days.	M		iv.	
126.	040606	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			
127.	040607	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			
128.	049900	CA-99	This is a blank formatting row.				
129.	050000	**PM-00**	***1.5 Information Security Program Management (PM) Family***				
130.	050100	**PM-01**	**1.5.1 PM-1 Information Security Program Plan** *[NIST 800-53, CMS MARS-E]*				
131.	050101	**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		i.	
132.	050102	**PM-01b**	b. Review the organization-wide information security program plan at an organization defined frequency.	M		a.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
133.	050103	PM-01c	c. Revise the plan to address organizational changes and problems identified during plan implementation or security control assessments.	M		b.	
134.	050200	PM-02	**1.5.2 PM-2 Senior Information Security Officer** *[NIST 800-53, CMS MARS-E]*				
135.	050201	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			
136.	050300	PM-03	**1.5.3 PM-3 Information Security Resources** *[NIST 800-53, CMS MARS-E]*				
137.	050301	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			
138.	050302	PM-03b	b. Employ a business case/Exhibit 300/Exhibit 53 to record the resources required.	M			
139.	050303	PM-03c	c. Ensure that information security resources are available for expenditure as planned.	M			
140.	050400	PM-04	**1.5.4 PM-4 Plan Of Action And Milestones Process** *[NIST 800-53, CMS MARS-E]*				
141.	050401	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		a.	
142.	050500	PM-05	**1.5.5 PM-5 Information System Inventory** *[NIST 800-53, CMS MARS-E]*				
143.	050501	PM-05a	a. The organization shall develop and maintain an inventory of its information systems.	M		a.	
144.	050600	PM-06	**1.5.6 PM-6 Info. Security Measures of Performance** *[NIST 800-53, CMS MARS-E]*				
145.	050601	PM-06a	a. The organization shall develop, monitor, and report on the results of information security measures of performance.	M		a.	
146.	050700	PM-07	**1.5.7 PM-7 Enterprise Architecture** *[NIST 800-53, CMS MARS-E]*				
147.	050701	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		a.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
148.	050800	PM-08	**1.5.8 PM-8 Critical Infrastructure Plan** *[NIST 800-53, CMS MARS-E]*				
149.	050801	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		a.	
150.	050900	PM-09	**1.5.9 PM-9 Risk Management Strategy** *[NIST 800-53, CMS MARS-E]*				
151.	050901	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		a.	
152.	050902	PM-09b	b. Implement that strategy consistently across the organization.	M		b.	
153.	051000	PM-10	**1.5.10 PM-10 Security Authorization Process**				
154.	051001	PM-10a	a. The organization: manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;	M		a.	
155.	051002	PM-10b	b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and	M		b.	
156.	051003	PM-10c	c. Fully integrates the security authorization processes into an organization-wide risk management program.	M		c.	
157.	051004	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.*				
158.	051100	PM-11	**1.5.11 PM-11 Mission/Business Process Definition**				
159.	051101	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		a.	
160.	051102	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		b.	
161.	051103	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			
162.	059900	PM-99	This is a blank formatting line.				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
163.	060000	**IA-00**	***1.6 Identification and Authentication (IA)***				
164.	060100	**IA-01**	**1.6.1 IA-1 – Identification& Authentication P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
165.	060101	IA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
166.	060102	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	In	a.	
167.	060103	IA-01b	b. Formal, documented **procedures** to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	L	P	b.	
168.	060200	**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]*				
169.	060201	IA-02a	The information system shall: a. Uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	M		i.	
170.	060202	IA-02b	b. Use **multifactor authentication** for network access to privileged accounts.	M		a.	
171.	060203	IA-02c	c. Use **multifactor authentication** for network access to non-privileged accounts.	M		b.	
172.	060204	IA-02d	d. Use **multifactor authentication** for local access to privileged accounts.	M		c.	
173.	060205	IA-02e	**e. Use replay resistant authentication mechanisms for network access to privileged accounts.**	M		d.	
174.	060206	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		e.	
175.	060300	**IA-03**	**1.6.3 IA-3 – Device Identification and Authentication [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
176.	060301	IA-03a	a. The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection.	M		i.	
177.	060400	**IA-04**	**1.6.4 IA-4 – Identifier Management [M]** *[NIST 800-53, CMS MARS-E]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
178.	060401	**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		a.	
179.	060402	**IA-04b**	b. Selecting an identifier that uniquely identifies an individual or device.	M		b.	
180.	060403	**IA-04c**	c. Assigning the user identifier to the intended party or the device identifier to the intended device.	M		c.	
181.	060404	**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		d.	
182.	060405	**IA-04e**	e. Disabling the user identifier after sixty (60) days or less and deleting disabled accounts during the annual re-certification process.	M		e.	
183.	060500	**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]*				
184.	060501	**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		i.	
185.	060502	**IA-05b**	b. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.	M		a.	
186.	060503	**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		*i.*	
187.	060504	**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			

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
188.	060505	**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			
189.	060506	**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		f.	
190.	060507	**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		g.	
191.	060508	**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		h.	
192.	060509	**IA-05i**	i. The information system shall routinely prompt users to change their passwords within 5-14 days before such password expires.	M		i.	
193.	060510	**IA-05j**	j. User account lockout feature shall disable the user account after 3 unsuccessful login attempts.	M		j.	
194.	060511	**IA-05k**	k. Account lockout duration shall be permanent until an authorized system administrator reinstates the user account.	M		k.	
195.	060512	**IA-05l**	l. Default vendor passwords shall be changed upon successful installation of the information system product.	M		l.	
196.	060513	**IA-05m**	m. System initialization (boot) settings shall be password-protected.	M		m.	
197.	060514	**IA-05n**	n. Clear-text representation of passwords shall be suppressed (blotted out) when entered at the login screen.	M		n.	
198.	060515	**IA-05o**	o. Passwords shall not be automated through function keys, scripts or other methods where passwords may be stored on the system.	M		o.	
199.	060516	**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		p.	
200.	060600	**IA-06**	**1.6.6 IA-6 – Authenticator Feedback [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
201.	060601	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		a.	
202.	060700	**IA-07**	**1.6.7 IA-7 – Cryptographic Module Authent. [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
203.	060701	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		a.	
204.	060800	**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]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
205.	060801	IA-08a	a. The information system shall uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	M	I	a.	
206.	069900	IA-99	This is a blank formatting line.				
207.	070000	**AC-00**	***1.7 AC – Access Control***				
208.	070100	**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]*				
209.	070101	AC-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
210.	070102	AC-01a	a. A formal, documented access control **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
211.	070103	AC-01b	b. Formal, documented **procedures** to facilitate the implementation of the access control policy and associated access controls.	L	P		
212.	070200	AC-02	**1.7.2 AC-2 – Account Management [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
213.	070201	AC-02a	a. The organization shall manage information system accounts, including:	M			
214.	070202	AC-02a1	i. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary).	M		i.	
215.	070203	AC-02a2	ii. Establishing conditions for group membership.	M		ii.	
216.	070204	AC-02a3	iii. Identifying authorized users of the information system and specifying access privileges.	M		iii.	
217.	070205	AC-02a4	iv. Requiring appropriate approvals for requests to establish accounts.	M		iv.	
218.	070206	AC-02a5	v. Establishing, activating, modifying, disabling, and removing accounts.	M		v.	
219.	070207	AC-02a6	vi. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts.	M		vi.	
220.	070208	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		vii.	
221.	070209	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		viii.	
222.	070210	AC-02a9	ix. Terminating emergency accounts within twenty-four (24) hours.	M		ix.	
223.	070211	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		x.	
224.	070212	AC-02a11	xi. Reviewing information system accounts within every one-hundred-eighty (180) days and requiring annual certification.	M		xi.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
225.	070213	AC-02a12	xii. Automatically audit account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	M		xii.	
226.	070214	AC-02.1	The organization employs automated mechanisms to support the management of information system accounts.	M			
227.	070215	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			
228.	070216	AC-02.3	The information system automatically disables inactive accounts after one hundred eighty (180) days.	M			
229.	070217	AC-02.4	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	M			
230.	070218	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		a.	
231.	070219	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		b.	
232.	070220	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		c.	
233.	070300	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]*				
234.	070301	AC-03a	a. The information system shall enforce approved authorizations for logical access to the system in accordance with applicable policy.	M		i.	
235.	070302	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			
236.	070400	AC-04	**1.7.4 AC-4 – Information Flow Enforcement [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
237.	070401	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		i.	
238.	070402	AC-04b	b. *[ISO 27001:2005]* Groups of information services, users, and information systems shall be segregated on networks.	M		a.	
239.	070403	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		b.	
240.	070404	AC-04d	d. Opportunities for information leakage shall be prevented.	M		c.	
241.	070500	AC-05	**1.7.5 AC-5 – Separation of Duties [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
242.	070501	AC-05a	The organization shall: a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.	M		a.	
243.	070502	AC-05b	b. Document separation of duties.	M		b.	
244.	070503	AC-05c	c. Implement separation of duties through assigned information system access authorizations.	M		c.	
245.	070600	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]*				
246.	070601	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 ARIES missions and business functions.	M		i.	
247.	070602	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			
248.	070603	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			
249.	070700	AC-07	**1.7.7 AC-7 – Unsuccessful Login Attempts [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
250.	070701	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		i.	
251.	070702	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		a.	
252.	070800	AC-08	**1.7.8 AC-8 – System Use Notification [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
253.	070801	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			
254.	070802	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		a.	
255.	070803	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		b.	
256.	070900	AC-10	**1.7.9 AC-10 – Concurrent Session Control [M]** *[NIST 800-53, CMS MARS-E]*				
257.	070901	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		a.	
258.	071000	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]*				
259.	071001	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			
260.	071002	AC-11b	b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.	M		a.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
261.	071100	AC-14	**1.7.11 AC-14 – Permitted Actions without Identification or Authentication [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
262.	071101	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		a.	
263.	071102	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		b.	
264.	071103	AC-14c	c. Permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	M		c.	
265.	071200	AC-17	**1.7.12 AC-17 – Remote Access [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
266.	071201	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			
267.	071202	AC-17a	**If authorized**, the organization shall: a. Document allowed methods of remote access to the information system.	M		a.	
268.	071203	AC-17b	b. Establish usage restrictions and implementation guidance for each allowed remote access method.	M		b.	
269.	071204	AC-17c	c. Monitor for unauthorized remote access to the information system.	M		c.	
270.	071205	AC-17d	d. Authorize remote access to the information system prior to connection.	M		d.	
271.	071206	AC-17e	e. Enforce requirements for remote connections to the information system.	M		e.	
272.	071207	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		f.	
273.	071208	AC-17g	g. The information system shall route all remote accesses through a limited number of managed access control points.	M		g.	
274.	071209	AC-17h	*[NIST 800-53]* The organization shall: h. Use cryptography to protect the confidentiality and integrity of remote access sessions.	M		h.	
275.	071210	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		i.	
276.	071211	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		j.	
277.	071212	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		k.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
278.	071213	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		l.	
279.	071214	AC-17m	m. ***[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		n.	
280.	071300	AC-18	**1.7.13 AC-18 – Wireless Access [M]** *[NIST 800-53, CMS MARS-E]*				
281.	071301	AC-18	The organization shall prohibit the installation of wireless access points (WAP) to ARIES information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization shall:	M			
282.	071302	AC-18a	a. Monitor for unauthorized wireless access to the information system.	M			
283.	071303	AC-18b	b. Enforce requirements for wireless connections to the information system.	M			
284.	071304	AC-18c	c. Protect wireless access to the system using authentication and encryption if wireless access is explicitly approved.	M			
285.	071305	AC-18d	[NIST 800-53, IRS 1075] The organization shall d. Establish policy, usage restrictions and implementation guidance for wireless access.	M			
286.	071306	AC-18e	e. Authorize wireless access to the information system prior to connection.	M			
287.	071400	AC-19	**1.7.14 AC-19 – Access Control for Mobile Devices [M]** *[NIST 800-53, CMS MARS-E]*				
288.	071401	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 ARIES information systems **unless explicitly authorized**, in writing, by the CIO or his/her designated representative. **If authorized, the organization shall:**	M			
289.	071402	AC-19a	a. Monitor for unauthorized connections of mobile devices to information systems.	M			
290.	071403	AC-19b	b. Enforce requirements for the connection of mobile devices to information systems.	M			
291.	071404	AC-19c	c. Disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.	M			
292.	071405	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			
293.	071406	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			

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
294.	071407	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			
295.	071408	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			
296.	071409	AC-19h	h. Restrict the use of writable, removable media in organizational information systems.	M			
297.	071410	AC-19i	i. Prohibit the use of personally owned, removable media in organizational information systems.	M			
298.	071411	AC-19j	j. Prohibit the use of removable media in organizational information systems when the media has no identifiable owner.	M			
299.	071412	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			
300.	071413	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			
301.	071500	AC-20	**1.7.15 AC-20 – Use of External Info. Systems [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
302.	071501	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			
303.	071502	AC-20a	a. The types of applications that can be accessed from external information systems.	M		a.	
304.	071503	AC-20b	**b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted.**	M		b. The FIPS 199 security category of information is medium.	
305.	071503	AC-20c	c. How other users of the external information system will be prevented from accessing federal information.	M		c.	
306.	071504	AC-20d	d. The use of virtual private networking (VPN) and firewall technologies.	M		d.	
307.	071505	AC-20e	e. The use of and protection against the vulnerabilities of **wireless** technologies.	M		e.	
308.	071506	AC-20f	f. The maintenance of adequate physical security controls.	M		f.	
309.	071507	AC-20g	g. The use of virus and spyware protection software.	M		g.	
310.	071508	AC-20h	h. How often the security capabilities of installed software are to be updated.	M		h.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
311.	071509	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			
312.	071510	AC-20.1b	b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system	M			
313.	071511	AC-20.2	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	M			
314.	071600	AC-22	**1.7.16 AC-22 – Publicly Accessible Content [M]** *[NIST 800-53, CMS MARS-E]*				
315.	071601	AC-22a	The organization shall: a. Designate individuals authorized to post information onto an organizational information system that is publicly accessible.	M			
316.	071602	AC-22b	b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	M			
317.	071603	AC-22c	c. Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.	M			
318.	071604	AC-22d	d. Review the content on the publicly accessible organizational information system for nonpublic information at an organization-defined frequency.	M			
319.	071605	AC-22e	e. Remove nonpublic information from the publicly accessible organizational information system, if discovered.	M			
320.	080000	**AU-00**	***1.8 Audit and Accountability (AU) Family***				
321.	080100	**AU-01**	**1.8.1 AU-1 – Audit and Accountability P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
322.	080101	**AU-01**	The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days:	L	P		
323.	080102	**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	In	a.	
324.	080103	**AU-01b**	b. Formal, documented **procedures** to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	L	P	b.	
325.	080200	**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]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
326.	080201	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		a.	
327.	080202	AU-02a1	i. Server alerts and error messages.	M			
328.	080203	AU-02a2	ii. User log-on and log-off (successful or unsuccessful).	M			
329.	080204	AU-02a3	iii. All system administration activities.	M			
330.	080205	AU-02a4	iv. Modification of privileges and access.	M			
331.	080206	AU-02a5	v. Start up and shut down.	M			
332.	080207	AU-02a6	vi. Application modifications.	M			
333.	080208	AU-02a7	vii. Application alerts and error messages.	M			
334.	080209		viii. Configuration changes.	M			
335.	080210	AU-02a9	ix. Account creation, modification, or deletion.	M			
336.	080211	AU-02a10	x. File creation and deletion.	M			
337.	080212	AU-02a11	xi. Read access to sensitive information.	M			
338.	080213	AU-02a12	xii. Modification to sensitive information.	M			
339.	080214	AU-02a13	xiii. Printing sensitive information.	M			
340.	080215	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		b.	
341.	080216	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		c.	
342.	080217	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		d.	
343.	080218	AU-02d1	See above.	M			
344.	080219	AU-02d2	See above.	M			
345.	080220	AU-02d3	See above.	M			
346.	080221	AU-02d4	See above.	M			
347.	080222	AU-02d5	See above.	M			
348.	080223	AU-02d6	See above.	M			
349.	080224	AU-02d7	See above.	M			
350.	080225	AU-02d8	See above.	M			

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
351.	280226	**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		e.	
352.	280227	**AU-02f**	f. Review and update the list of auditable events at an organization-defined frequency.	M		f.	
353.	280300	**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]*				
354.	280301	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		i.	
355.	280302	**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		a.	
356.	280400	**AU-04**	**1.8.4 AU-4 – Audit Storage Capacity [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
357.	280401	**AU-04a**	a. The organization shall allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.	M		a.	
358.	280500	**AU-05**	**1.8.5 AU-5 – Response to Audit Failures [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
359.	280501	**AU-05a**	The information system shall: a. Alert designated organizational officials in the event of an audit processing failure.	M		a.	
360.	280502	**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		b.	
361.	280600	**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]*				
362.	280601	**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		a.	
363.	280602	**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		b.	
364.	280603	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			

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
365.	080700	AU-07	**1.8.7 AU-7 – Audit Reduction and Report Generation [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
366.	080701	AU-07a	a. The information system shall provide an audit reduction and report generation capability.	M		a.	
367.	080702	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		b.	
368.	080800	AU-08	**1.8.8 AU-8 – Time Stamps [M]** *[NIST 800-53, CMS MARS-E, IRS 1075, SSA System Security Guidelines]*				
369.	080801	AU-08a	a. The information system shall use internal system clocks to generate time stamps for audit records.	M		a.	
370.	080802	AU-08b	b. The information system shall synchronize internal information system clocks daily and at system boot.	M		b.	
371.	080900	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]*				
372.	080901	AU-09a	a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.	M		a.	
373.	081000	AU-10	**1.8.10 AU-10 – Non-Repudiation [M]** *[NIST 800-53, CMS MARS-E]*				
374.	081001	AU-10a	a. The information system shall protect against an individual falsely denying having performed a particular action.	M		a.	
375.	081100	AU-11	**1.8.11 AU-11 – Audit Record Retention [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
376.	081101	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		a.	
377.	081102	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		b.	
378.	081103	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		c.	
379.	081104	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		d.	
380.	081105	AU-11e	e. Audit file data shall be unalterable (read only) and maintained for a minimum of three (preferably seven) years.	M		e.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
381.	081200	AU-12	**1.8.12 AU-12 – Audit Generation [M]** *[NIST 800-53, The Patient Protection and Affordable Care Act, CMS MARS-E, HITECH]*				
382.	081201	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		i.	
383.	081202	AU-12a2	ii. All changes to logical access control authorities (e.g., rights, permissions).	M		ii.	
384.	081203	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		iii.	
385.	081204	AU-12a4	iv. The audit trail shall capture the enabling or disabling of audit report generation services.	M		iv.	
386.	081205	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		v.	
387.	081206	AU-12b	b. Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system.	M		a.	
388.	081207	AU-12c	c. Generate audit records for the list of audited events.	M		b.	
389.	081208	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		c.	
390.	081209	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		d.	
391.	089900	AU-99	This is a blank formatting row.				
392.	090000	SC-00	***1.9 System and Communications Protection (SC) Family***				
393.	090100	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]*				
394.	090101	SC-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
395.	090102	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	In	a.	
396.	090103	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	P	b.	
397.	090104	SC-01c	c. *[ISO 27001:2005]* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	L	In	c.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
398.	290200	SC-02	**1.9.2 SC-2 – Application Partitioning [M]** *[NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]*				
399.	290201	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		a.	
400.	290300	SC-04	**1.9.3 SC-4 – Information in Shared Resources [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
401.	290301	SC-04a	a. The information system shall prevent unauthorized and unintended information transfer via shared system resources.	M			
402.	290400	SC-05	**1.9.4 SC-5 – Denial of Service Protection [M]** *[NIST 800-53, CMS MARS-E]*				
403.	290401	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		a.	
404.	290402	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		b.	
405.	290403	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		c.	
406.	290500	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]*				
407.	290501	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		a.	
408.	290502	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		b.	
409.	290503	SC-07c	c. Physically allocate publicly accessible information system components to separate sub-networks with separate physical network interfaces.	M		c.	
410.	290504	SC-07d	d. Prevent public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	M		d.	
411.	290505	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		e.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
412.	090506	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		i.	
413.	090600	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]*				
414.	090601	SC-08a	a. The information system shall protect the integrity of transmitted information.	M			
415.	090602	SC-08b	b. The organization shall employ cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	M			
416.	090700	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]*				
417.	090701	SC-09a	a. The information system shall protect the confidentiality of transmitted information.	M			
418.	090702	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			
419.	090800	SC-10	**1.9.8 SC-10 – Network Disconnect [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
420.	090801	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		a.	
421.	090802	SC-10b	b. Forcibly disconnect inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity.	M		b.	
422.	090900	SC-12	**1.9.9 SC-12 – Cryptographic Key Establishment and Management [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
423.	090901	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		a.	
424.	090902	SC-12b	b. *[IRS 1075]* The organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	M		b.	
425.	091000	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]*				
426.	091001	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		a.	
427.	091002	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		b.	
428.	091003	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		c.	
429.	091004	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		d.	
430.	091100	SC-14	**1.9.11 SC-14 – Public Access Protections [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
431.	091101	SC-14a	a. The information system shall protect the integrity and availability of publicly available information and applications.	M			
432.	091200	SC-15	**1.9.12 SC-15 – Collaborative Computing Devices [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
433.	091201	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			
434.	091202	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			
435.	091300	SC-17	**1.9.13 SC-17 – Public Key Infrastructure Certs [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
436.	091301	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			
437.	091302	SC-17b	b. *[IRS 1075]* The agency shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	M			
438.	091400	SC-18	**1.9.14 SC-18 – Mobile Code [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
439.	091401	SC-18a	The organization shall: a. Define acceptable and unacceptable mobile code and mobile code technologies.	M			
440.	091402	SC-18b	b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.	M			
441.	091403	SC-18c	c. Authorize, monitor, and control the use of mobile code within the information system.	M			
442.	091500	SC-19	**1.9.15 SC-19 – Voice Over Internet Protocol [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
443.	091501	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			
444.	091502	SC-19b	b. Authorize, monitor, and control the use of VoIP within the information system.	M			
445.	091600	SC-20	**1.9.16 SC-20 – Secure Name Resouce Svc. (Auth Source) [M]** *[NIST 800-53, CMS MARS-E]*				
446.	091601	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			
447.	091602	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			
448.	091700	SC-22	**1.9.17 SC-22 – Architecture for Name Res. Svc. [M]** *[NIST 800-53, CMS MARS-E]*				
449.	091701	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		i.	
450.	091800	SC-23	**1.9.18 SC-23 – Session Authenticity [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
451.	091801	SC-23a	a. The information system shall provide mechanisms to protect the authenticity of communications sessions.	M		i.	
452.	091900	SC-28	**1.9.19 SC-28 – Protection of Information at Rest [M]** *[NIST 800-53, CMS MARS-E]*				
453.	091901	SC-28a	a. The information system shall protect the confidentiality and integrity of information at rest.	M		a.	
454.	092000	SC-32	**1.9.20 SC-32 – Information System Partitioning [M]** *[NIST 800-53, Medicaid Information Tech Architecture, CMS MARS-E]*				
455.	092001	SC-32a	a. The organization shall partition the information system into components residing in separate physical domains (or environments) as deemed necessary.	M		a.	
456.	092100	SC-66	**1.9.21 SC-ACA-1 – Electronic Mail [M]-1 – Electronic Mail [M]**				
457.	092101	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			
458.	099900	SC-99	This is a blank formatting line				
459.	100000	PS-00	***1.10 Personnel Security (PS) Family***				
460.	100100	PS-01	**1.10.1 PS-1 – Personnel Security P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
461.	100101	PS-01	The organization shall develop, disseminate, and review/update within every three hundred sixty-five (365) days:	L	P		
462.	100102	PS-01a	a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
463.	100103	PS-01b	b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	L	P	b.	
464.	100104	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	I	c.	
465.	100105	PS-01d	d. To determine that the access of a workforce member to electronic protected health information is appropriate.	L	I	d.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
466.	100200	PS-02	**1.10.2 PS-2 – Position Categorization [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
467.	100201	PS-02a	The organization shall: a. Assign a criticality/sensitivity risk designation to all positions.	L		i.	
468.	100202	PS-02b	b. Establish screening criteria for individuals filling those positions.	L			
469.	100203	PS-02c	c. Review and revise position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.	L		a.	
470.	100300	PS-03	**1.10.3 PS-3 – Personnel Screening [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
471.	100301	PS-03a	a. The organization shall: Screen individuals prior to authorizing access to the information system.	M		i.	
472.	100302	PS-03b	b. Rescreen individuals periodically, consistent with the criticality/sensitivity rating of the position.	M		a.	
473.	100400	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]*				
474.	100401	PS-04a	The organization, upon termination of individual employment shall: a. Revoke system and physical access immediately following employee termination.	M			
475.	100402	PS-04b	b. Conduct exit interviews.	M		a.	
476.	100403	PS-04c	c. Retrieve all security-related information system-related property.	M		b.	
477.	100404	PS-04d	d. Retain access to information and information systems formerly controlled by terminated individual.	M		c.	
478.	100405	PS-04e	e. Immediately escort employees terminated for cause out of the organization.	M		d.	
479.	100406	PS-04f	*[ISO 27001:2005]* f. Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	M		e.	
480.	100500	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]*				
481.	100501	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		i.	
482.	100502	PS-05b	b. Notification to security management.	M		b.	
483.	100503	PS-05c	c. Closing obsolete accounts and establishing new accounts.	M		i.	
484.	100504	PS-05d	d. Revocation of all system access privileges (if applicable).	M			
485.	100600	PS-06	**1.10.6 PS-6 – Access Agreements [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
486.	100601	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		a.	
487.	100602	PS-06b	b. Review/update the access agreements as part of the system security authorization or when a contract is renewed or extended.	M		b.	
488.	100700	PS-07	**1.10.7 PS-7 – Third-Party Personnel Security [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
489.	100701	PS-07a	The organization shall: a. Establish personnel security requirements including security roles and responsibilities for third-party providers.	M		a.	
490.	100702	PS-07b	b. Document personnel security requirements.	M		b.	
491.	100703	PS-07c	c. Monitor provider compliance.	M		c.	
492.	100800	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]*				
493.	100801	PS-08a	a. The organization shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.	M		a.	
494.	100900	PS-99	This line is a blank formatting line.				
495.	110000	PE-00	***1.11 Physical and Environmental Protection (PE) Family***				
496.	110100	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]*				
497.	110101	PE-01	The organization shall develop, disseminate, and review/update within every three hundred sixty-five (365) days:	L	P		
498.	110102	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	In	a.	
499.	110103	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	P	b.	
500.	110200	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]*				
501.	110201	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		a.	
502.	110202	PE-02b	b. Issue authorization credentials.	M		b.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
503.	110203	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		c.	
504.	110300	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]*				
505.	110301	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			
506.	110302	PE-03b	b. Verify individual access authorizations before granting access to the facility.	M		b.	
507.	110303	PE-03c	c. Control entry to the facility containing the information system using physical access devices and/or guards.	M			
508.	110304	PE-03d	d. Control access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.	M		d.	
509.	110305	PE-03e	e. Secure keys, combinations, and other physical access devices.	M		e.	
510.	110306	PE-03f	f. Inventory physical access devices within every three hundred sixty-five (365) days.	M		f.	
511.	110307	PE-03g	g. Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.	M		i.	
512.	110308	PE-03h	h. *[ISO 27001:2005]* Physical protection and guidelines for working in secure areas shall be designed and applied.	M		g.	
513.	110309	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		h.	
514.	110310	PE-03j	j. The agency shall issue authorization credentials to include badges, identification cards and/or smart cards.	M		i.	
515.	110400	PE-04	**1.11.4 PE-4 – Access Control for Transmission Medium [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
516.	110401	PE-04a	a. The organization shall control physical access to information system distribution and transmission lines within organizational facilities.	M		a.	
517.	110402	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		b.	
518.	110403	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		c.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
519.	110500	PE-05	**1.11.5 PE-5 – Access Control for Output Devices [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
520.	110501	PE-05a	a. The organization shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	M			
521.	110600	PE-06	**1.11.6 PE-6 – Monitoring Physical Access [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
522.	110601	PE-06a	The organization shall: a. Monitor physical access to the information system to detect and respond to physical security incidents.	M		a.	
523.	110602	PE-06b	b. Review physical access logs at least semi-annually.	M		b.	
524.	110603	PE-06c	c. Coordinate results of reviews and investigations with the organization's incident response capability.	M		c.	
525.	110604	PE-06d	d. Monitor real-time physical intrusion alarms and surveillance equipment.	M		d.	
526.	110700	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]*				
527.	110701	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			
528.	110702	PE-07b	b. Escort visitors and monitor visitor activity, when required.	M		a.	
529.	110800	PE-08	**1.11.8 PE-8 – Access Records [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
530.	110801	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		a.	
531.	110802	PE-08b	b. Review visitor access records monthly.	M		b.	
532.	110803	PE-08c	c. ***[IRS 1075]*** When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure.	M		c.	
533.	110804	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		d.	
534.	110805	PE-08e	e. Designated officials or designees within the organization shall review the visitor access records, at least annually.	M		e.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
535.	110806	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		f.	
536.	110900	PE-09	**1.11.9 PE-9 – Power Equipment and Cabling [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
537.	110901	PE-09a	a. The organization shall protect power equipment and power cabling for the information system from damage and destruction.	M		a.	
538.	111000	PE-10	**1.11.10 PE-10 – Emergency Shutoff [M]** *[NIST 800-53, CMS MARS-E]*				
539.	111001	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		a.	
540.	111002	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		b.	
541.	111003	PE-10c	c. Protect emergency power shutoff capability from unauthorized activation.	M		c.	
542.	111100	PE-11	**1.11.11 PE-11 – Emergency Power [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
543.	111101	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		a.	
544.	111200	PE-12	**1.11.12 PE-12 – Emergency Lighting [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
545.	111201	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		a.	
546.	111300	PE-13	**1.11.13 PE-13 – Fire Protection [M]** [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
547.	111301	PE-13a	The organization shall: a. Employ and maintain fire suppression and detection devices/systems for the information system.	M		i.	
548.	111302	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		a.	
549.	111303	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		i.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
550.	111304	PE-13d	d. Employ automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	M		d.	
551.	111400	PE-14	**1.11.14 PE-14 – Temp. and Humidity Controls [M]** *[NIST 800-53, CMS MARS-E]*				
552.	111401	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		a.	
553.	111402	PE-14b	b. Monitor temperature and humidity levels.	M		b.	
554.	111500	PE-15	**1.11.15 PE-15 – Water Damage Protection [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
555.	111501	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		a.	
556.	111600	PE-16	**1.11.16 PE-16 – Delivery and Removal [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
557.	111601	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		a.	
558.	111700	PE-17	**1.11.17 PE-17 – Alternate Work Site [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
559.	111701	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		i.	
560.	111702	PE-17b	b. Assess as feasible, the effectiveness of security controls at alternate work sites.	M		b.	
561.	111703	PE-17c	c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.	M		c.	
562.	111800	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]*				
563.	111801	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.			i.	
564.	111802	PE-99	This is a blank formatting row.				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
565.	120000	**CP-00**	***1.12 Contingency Planning (CP) Family***				
566.	120100	**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]*				
567.	120101	**CP-01**	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
568.	120102	**CP-01a**	a. A formal, documented contingency planning **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
569.	120103	**CP-01b**	b. Formal, documented **procedures** to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	L	P	b.	
570.	120200	**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]*				
571.	120201	**CP-02a**	The organization shall: a. Develop a Contingency Plan (CP) for the information system that: i. Identifies essential ARIES 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		i.	
572.	120202	**CP-02b**	b. Distribute copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements.	M			
573.	120203	**CP-02c**	c. Coordinate contingency planning activities with incident handling activities.	M		a.	
574.	120204	**CP-02d**	d. Review the CP for the information system within every three-hundred-sixty-five (365) days.	M			
575.	120205	**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		b.	
576.	120206	**CP-02f**	f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements.	M		c.	
577.	120207	**CP-02.1**	How does the organization coordinate contingency plan development with organizational elements responsible for related plans?	M			
578.	120208	**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			

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
579.	120300	CP-03	**1.12.3 CP-3 – Contingency Training [M]** *[NIST 800-53, CMS MARS-E]*				
580.	120301	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			
581.	120400	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]*				
582.	120401	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			
583.	120500	CP-06	**1.12.5 CP-6 – Alternate Storage Site [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
584.	120501	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		a.	
585.	120502	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		b.	
586.	120503	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		c.	
587.	120600	CP-07	**1.12.6 CP-7 – Alternate Processing Site [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
588.	120601	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		a.	
589.	120602	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		b.	
590.	120603	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		c.	
591.	120604	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		d.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
592.	120605	CP-07e	e. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	M		e.	
593.	120606	CP-07f	f. Ensure that the alternate processing site provides information security measures equivalent to that of the primary site.	M		f.	
594.	120700	CP-08	**1.12.7 CP-8 – Telecommunications Services [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
595.	120701	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		a.	
596.	120702	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		b.	
597.	120703	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		c.	
598.	120704	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		d.	
599.	120800	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]*				
600.	120801	CP-09a	The organization shall: a. Conduct weekly backups of user-level information contained in the information system.	M			
601.	120802	CP-09b	b. Conduct weekly backups of system-level information contained in the information system.	M			
602.	120803	CP-09c	c. Conduct backups of information system documentation including security-related documentation and other forms of data, including paper records.	M		c.	
603.	120804	CP-09d	d. Protect the confidentiality and integrity of ARIES system backup information at the storage location.	M		d.	
604.	120805	CP-09e	e. Test backup information following each backup to verify media reliability and information integrity.	M		e.	
605.	120806	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		f.	
606.	120900	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]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
607.	120901	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		i.	
608.	120902	CP-10b	b. The information system shall implement transaction recovery for systems that are transaction-based.	M		a.	
609.	120903	CP-10c	c. The organization shall provide Compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.	M		b.	
610.	129900	CP-99	This is a blank formatting line.				
611.	130000	CM-00	***1.13 Configuration Management (CM)***				
612.	130100	CM-01	**1.13.1 CM-1 – Configuration Management P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
613.	130101	CM-01	The organization shall develop, disseminate, and review/update within every three-hundred sixty-five (365) days:	L	P		
614.	130102	CM-01a	a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	I	a.	
615.	130103	CM-01b	b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	L	P	b.	
616.	130200	CM-02	**1.13.2 CM-2 – Baseline Configuration [M]** *[NIST 80-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
617.	130201	CM-02a	The organization shall: a. Develop, document, and maintain under configuration control, a current baseline configuration of the information system.	M		a.	
618.	130202	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		i.	
619.	130203	CM-02c	c. Retain older versions of baseline configurations as deemed necessary to support rollback.	M		b.	
620.	130204	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		c.	
621.	130205	CM-02e	e. Employ an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.	M		d.	
622.	130300	CM-03	**1.13.3 CM-3 – Configuration Change Control [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
623.	130301	**CM-03a**	The organization shall: a. Determine the types of changes to the information system that are configuration controlled.	M		a.	
624.	130302	**CM-03b**	b. Approve configuration-controlled changes to the system with explicit consideration for security impact analyses.	M		b.	
625.	130303	**CM-03c**	c. Document approved configuration-controlled changes to the system.	M		c.	
626.	130304	**CM-03d**	d. Retain and review records of configuration-controlled changes to the system.	M		d.	
627.	130305	**CM-03e**	e. Audit activities associated with configuration-controlled changes to the system.	M		*e.*	
628.	130306	**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			
629.	130307	**CM-03g**	g. Test, validate, and document changes to the information system before implementing the changes on the operational system.	M		f.	
630.	130400	**CM-04**	**1.13.4 CM-4 – Security Impact Analysis [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
631.	130401	**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		a.	
632.	130402	**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		b.	
633.	130403	**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			
634.	130404	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		a.	
635.	130500	**CM-05**	**1.13.5 CM-5 – Access Restrictions for Change [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
636.	130501	**CM-05a**	a. The organization shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	M			
637.	130502	**CM-05a2**	Continued from above.				
638.	130600	**CM-06**	**1.13.6 CM-6 – Configuration Settings [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
639.	130601	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			
640.	130602	CM-06b	b. Implement the configuration settings.	M		a.	
641.	130603	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		b.	
642.	130604	CM-06d	d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	M		c.	
643.	130605	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		d.	
644.	130700	CM-07	**1.13.7 CM-7 – Least Functionality [M]** *[NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]*				
645.	130701	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		a.	
646.	130702	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		b.	
647.	130800	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]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
648.	130801	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		i.	
649.	130802	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		a.	
650.	130803	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		b.	
651.	130900	CM-09	**1.13.9 CM-9 – Configuration Management Plan [M]** *[NIST 800-53, CMS MARS-E]*				
652.	130901	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		i.	
653.	130902	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			
654.	130903	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		See above.	
655.	139900	CM-99	Blank formatting line.				
656.	140000	MA-00	***1.14 Maintenance (MA) Family***				
657.	140100	MA-01	**1.14.1 MA-1 – System Maintenance P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
658.	140101	MA-01	The organization shall develop, disseminate, and review/update within every three hundred sixty-five (365) days:	L	P		
659.	140102	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	In	a.	
660.	140103	MA-01b	b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	L	P	b.	
661.	140200	MA-02	**1.14.2 MA-2 – Controlled Maintenance [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
662.	140201	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		a.	
663.	140202	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		b.	
664.	140203	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		c.	
665.	140204	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		d.	
666.	140205	MA-02e	e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	M		e.	
667.	140206	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		i.	
668.	140300	MA-03	**1.14.3 MA-3 – Maintenance Tools [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
669.	140301	MA-03a	The organization shall: a. Approve, control, monitor the use of, and maintain on an ongoing basis, information system maintenance tools.	M		a.	
670.	140302	MA-03b	b. Inspect all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.	M		b.	
671.	140303	MA-03c	c. Check all media containing diagnostic and test programs for malicious code before the media is used in the information system.	M		c.	
672.	140400	MA-04	**1.14.4 MA-4 – Non-Local Maintenance [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
673.	140401	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			
674.	140402	MA-04a	a. **Monitor** and control non-local maintenance and diagnostic activities. *(CMS clarification: who authorizes and who maintains the authorization document.)*	M		a.	
675.	140403	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		b.	
676.	140404	MA-04c	c. Employ **strong identification and authentication** techniques in the establishment of non-local maintenance and diagnostic sessions.	M		c.	
677.	140405	MA-04d	d. Maintain records for non-local maintenance and diagnostic activities.	M		d.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
678.	140406	MA-04e	e. Terminate all sessions and network connections when non-local maintenance is completed.	M		e.	
679.	140407	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		f.	
680.	140408	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		g.	
681.	140409	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		h.	
682.	140410	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		i.	
683.	140500	MA-05	**1.14.5 MA-5 – Maintenance Personnel [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				
684.	140501	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		a.	
685.	140502	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		b.	
686.	140600	MA-06	**1.14.6 MA-6 – Timely Maintenance [M]** *[NIST 800-53, CMS MARS-E]*				
687.	140601	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		a.	
688.	149900	MA-99	This is a blank formatting row.				
689.	150000	SI-00	***1.15 System and Information Integrity (SI)***				
690.	150100	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]*				
691.	150101	SI-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
692.	150302	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	I	a.	
693.	150303	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	P	b.	
694.	150200	SI-02	**1.15.2 SI-2 – Flaw Remediation [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
695.	150201	SI-02a	The organization shall: a. Identify, report, and correct information system flaws.	M			
696.	150202	SI-02b	b. Test software updates related to flaw remediation for effectiveness and potential side effects on information systems before installation.	M			
697.	150203	SI-02c	c. Incorporate flaw remediation into the organizational configuration management process.	M		c.	
698.	150204	SI-02d	d. Centrally manage the flaw remediation process and install software updates automatically.	M		d.	
699.	150205	SI-02e	e. Employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.	M		e.	
700.	150300	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]*				
701.	150301	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			
702.	150302	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		a.	
703.	150303	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			
704.	150304	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		d.	
705.	150305	SI-03e	e. Centrally manage malicious code protection mechanisms.	M		e.	
706.	150306	SI-03f	f. Ensure that the information system automatically updates malicious code protection mechanisms (including signature definitions).	M		f.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
707.	150307	SI-03g	g. Ensure that the information system prevents non-privileged users from circumventing malicious code protection capabilities.	M		g.	
708.	150308	SI-03h	h. *[ISO 27001:2005]* The organization shall implement appropriate user awareness procedures.	M		h.	
709.	150400	SI-04	**1.15.4 SI-4 – Information System Monitoring [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
710.	150401	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		a.	
711.	150402	SI-04b	b. Identify unauthorized use of the ARIES system.	M		b.	
712.	150403	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		c.	
713.	150404	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		d.	
714.	150405	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		e.	
715.	150406	SI-04f	f. Interconnect and configure individual intrusion detection tools into a system wide intrusion detection system using common protocols.	M		f.	
716.	150407	SI-04g	g. Employ automated tools to support near real-time analysis of events.	M		g.	
717.	150408	SI-04h	h. Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.	M		h.	
718.	150409	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		i.	
719.	150410	SI-04j	j. Ensure that the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	M		i.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
720.	150411	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		i.	
721.	150500	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]*				
722.	150501	SI-05a	The organization shall: a. Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.	M		a.	
723.	150502	SI-05b	b. Generate internal security alerts, advisories, and directives as deemed necessary.	M		b.	
724.	150503	SI-05c	c. Disseminate security alerts, advisories, and directives to appropriate personnel.	M		c.	
725.	150504	SI-05d	d. Implement security directives in accordance with established time frames, or notifies the degree of noncompliance.	M		d.	
726.	150600	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]*				
727.	150601	SI-07a	a. The information system shall detect unauthorized changes to software and information.	M			
728.	150602	SI-07b	b. The organization shall reassess the integrity of software and information by performing daily integrity scans of the information system.	M		a.	
729.	150603	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		i.	
730.	150700	SI-08	**1.15.7 SI-8 – Spam Protection [M]** *[NIST 800-53, CMS MARS-E]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
731.	150701	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			
732.	150702	SI-08b	b. Update spam protection mechanisms (including signature definitions) when new releases are available in accordance with configuration management policy and procedures.	M			
733.	150703	SI-08c	c. Centrally manage spam protection mechanisms.	M			
734.	150704	SI-08.1	SI-8(1) – Enhancement [M] Control The organization centrally manages spam protection mechanisms.	M			
735.	150800	SI-09	**1.15.8 SI-9 – Information Input Restrictions [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
736.	150801	SI-09a	a. The organization shall restrict the capability to input information to the information system to authorized personnel.	M		a.	
737.	150900	SI-10	**1.15.9 SI-10 – Information Input Validation [M]** *[NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E]*				
738.	150901	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		i.	
739.	151100	SI-11	**1.15.10 SI-11 – Error Handling [M]** *[NIST 800-53, CMS MARS-E]*				
740.	151101	SI-11a	The information system shall: a. Identify potentially security-relevant error conditions.	M			
741.	151102	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			
742.	151103	SI-11c	c. Reveal error messages only to authorized personnel.	M			
743.	151200	SI-12	**1.15.11 SI-12 – Information Output Handling and Retention [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
744.	151201	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		a.	
745.	159900	SI-99	This is a blank formatting line				
746.	160000	MP-00	***1.16 Media Protection (MP) Family***				
747.	160100	MP-01	**1.16.1 MP-1 – Media Protection P&P [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
748.	160101	**MP-01**	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
749.	160102	**MP-01a**	a. A formal, documented media protection **policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
750.	160103	**MP-01b**	b. Formal, documented **procedures** to facilitate the implementation of the media protection policy and associated media protection controls.	L	P	b.	
751.	160104	**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	In	c.	
752.	160200	**MP-02**	**1.16.2 MP-2 – Media Access [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
753.	160201	**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		a.	
754.	160202	**MP-02b**	b. Employ automated mechanisms to audit access attempts and access granted.	M		b.	
755.	160300	**MP-03**	**1.16.3 MP-3 – Media Marking [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
756.	160301	**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			
757.	160302	**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			
758.	160400	**MP-04**	**1.16.4 MP-4 – Media Storage [M]**				
759.	160401	**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		a.	
760.	160402	**MP-04b**	b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	M		b.	
761.	160500	**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]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
762.	160501	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			
763.	160502	MP-05b	b. Maintain accountability for information system media during transport outside of controlled areas.	M			
764.	160503	MP-05c	c. Restrict the activities associated with transport of such media to authorized personnel.	M			
765.	160504	MP-05d	d. Document activities associated with the transport of information system media.	M			
766.	160505	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			
767.	160600	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]*				
768.	160601	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		a.	
769.	160602	MP-06b	b. Employ sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	M		b.	
770.	160603	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		i.	
771.	160604	MP-06.1	Describe how the organization tracks, documents, and verifies media sanitization and disposal actions.	M			
772.	160605	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			
773.	160606	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			
774.	160607	MP-06.6	Describe the organization's process for destroying media containing sensitive information that cannot be sanitized.	M			
775.	160700	MP-07	**1.16.7 MP-ACA-1 – Media Related Records [M]** *[CMS MARS-E]*				
776.	160701	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		i.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
777.	169900	**MP-99**	This is a blank formatting row.				
778.	170000	**IR-00**	***1.17 Incident Response (IR) Family***				
779.	170100	**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]*				
780.	170101	IR-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
781.	170102	IR-01a	a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
782.	170103	IR-01b	b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	L	P	b.	
783.	170200	**IR-02**	**1.17.2 IR-2 – Incident Response Training [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
784.	170201	IR-02a	The organization shall: a. Train personnel in their incident response roles and responsibilities with respect to the information system.	M		a.	
785.	170201	IR-02b	b. Provide refresher training within every three-hundred-sixty-five (365) days.	M		b.	
786.	170300	**IR-03**	**1.17.3 IR-3 – Incident Response Exercises [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
787.	170301	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		i.	
788.	170400	**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]*				
789.	170401	IR-04a	The organization shall: a. Implement an incident handling capability using Information Security Incident Handling and Breach Notification Procedures.	M			
790.	170402	IR-04b	b. Coordinate incident handling activities with contingency planning activities.	M		a.	
791.	170403	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		b.	
792.	170404	IR-04d	d. Employ automated mechanisms to support the incident handling process.	M		c.	
793.	170405	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		d.	
794.	170500	**IR-05**	**1.17.5 IR-5 – Incident Monitoring [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
795.	170501	IR-05a	a. The organization tracks and documents information system security incidents.	M		a.	
796.	170600	**IR-06**	**1.17.6 IR-6 – Incident Reporting [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E, HIPAA]*				
797.	170601	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			
798.	170602	IR-06b	b. Report security incident information to designated authorities.	M			
799.	170603	IR-06c	c. The organization shall employ automated mechanisms to assist in the reporting of security incidents.	M		c.	
800.	170604	IR-06.1	The organization employs automated mechanisms to assist in the reporting of security incidents.	M			
801.	170700	**IR-07**	**1.17.7 IR-7 – Incident Response Assistance [M]** *[NIST 800-53, ISO 27001:2005, CMS MARS-E]*				
802.	170701	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		a.	
803.	170702	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		b.	
804.	170800	**IR-08**	**1.17.8 IR-8 – Incident Response Plan [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
805.	170801	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			
806.	170802	IR-08b	b. Distribute copies of the incident response plan to incident response personnel and organizational elements.	M		a.	
807.	170803	IR-08c	c. Review the incident response plan within every three-hundred-sixty-five (365) days.	M		b.	
808.	170804	IR-08d	d. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	M		c.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
809.	170805	IR-08e	e. Communicate incident response plan changes to incident response personnel and organizational elements.	M		d.	
810.	179908	**IR-99**	This is a blank formatting row.				
811.	180000	**AT-00**	***1.18 Awareness and Training (AT) Family***				
812.	180100	**AT-01**	**1.18.1 AT-1 – Security Awareness Training P&P [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
813.	180101	AT-01	The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:	L	P		
814.	180102	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	In	a.	
815.	180103	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	P	b.	
816.	180200	**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]*				
817.	180201	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			
818.	180202	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		a.	
819.	180203	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		b.	
820.	180204	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		c.	
821.	180205	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		e.	

RN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
822.	180300	**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]*				
823.	180301	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			
824.	180302	AT-03a2		M			
825.	180303	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			
826.	180304	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			
827.	180400	**AT-04**	**1.18.4 AT-4 – Security Training Records [M]** *[NIST 800-53, CMS MARS-E, IRS 1075]*				
828.	180401	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			
829.	180402	AT-04b	b. Retain individual training records for three (3) years.	M		b.	
830.	189900	AT-99	This is a blank formatting line.				
831.	200003	zz-99	☐			☐	