

State of Alaska  
Department of Health and Social Services

# **[system name] Security Plan**

# Table of Contents

1	Purpose of Document.....	8
2	Contact Information .....	8
2.1	System Name.....	8
2.2	Responsible Organization .....	8
2.3	System Owner.....	8
2.4	System Owner Designee.....	8
2.5	Program Manager .....	8
2.6	Program Manager .....	8
2.7	Security Plan Document Owner .....	8
2.8	Security Designee .....	8
2.9	Vendor Contact .....	8
2.10	Primary Technical Contact .....	8
2.11	Other Contacts .....	8
2.12	Other Contacts .....	8
3	Information Classification .....	9
3.1	System Categorization .....	9
3.2	Data Classification.....	9
3.3	Laws, Statutes, & Regulations Governing Information .....	9
3.4	Agreements with other parties (Business).....	9
4	Description of System.....	10
4.1	The function or purpose of the system and the information processed. (Business) ..	10
4.2	Business process description and diagram (Business) .....	10
4.3	List organizations which use data and how they use it. (Business).....	10
4.4	System IT Environment (IT) .....	10
4.5	Network Diagrams (IT-NS) .....	10
4.6	List of all linked or dependent applications (IT-BA) .....	11
4.6.1	Referenced Enterprise Services.....	11
4.7	List of Servers and IP addresses (IT-NS).....	11
4.8	List of IP Subnets, Routers, Firewalls (IT-NS) .....	11
4.9	List of Databases (IT-BA) .....	11
4.10	System Operational Status.....	12
4.11	System Vulnerability Scans and Continuous Monitoring .....	12
4.12	Patching and Support.....	12
4.13	Software Development Environments .....	12
4.14	Information Sensitivity .....	13
5	Risk Assessment.....	13
5.1	Information Sensitivity .....	13
5.2	Risk Analysis.....	13
5.3	Risk Assumption.....	13
6	Contingency Planning.....	13
6.1	Continuity of Operations Plan (COOP).....	13
6.2	Disaster Recovery (IT) .....	13
6.2.1	Backups (IT-NS).....	13
6.2.2	Other Recovery processes.....	13

[sysname] Security Plan

7	NIST 800-53+ Moderate System Controls.....	15
7.1	Risk Assessment (RA) Family.....	15
7.1.1	RA-1 – Risk Assessment P&P [M] .....	15
7.1.2	RA-2 – Security Categorization [M] .....	16
7.1.3	RA-3 – Risk Assessment [M].....	16
7.1.4	RA-5 – Vulnerability Scanning [M].....	16
7.2	Planning (PL) Family .....	17
7.2.1	PL-1 – Security Planning P&P [M].....	17
7.2.2	PL-2 – System Security Plan (SSP) [M] .....	17
7.2.3	PL-4 – Rules of Behavior (ROB) [M] .....	18
7.2.4	PL-5 – Privacy Impact Assessment (PIA) [M].....	18
7.2.5	PL-6 – Security-Related Activity Planning [M] .....	18
7.3	System and Services Acquisition (SA) .....	19
7.3.1	SA-1 – System& Services Acquisition P&P [M].....	19
7.3.2	SA-2 – Allocation of Resources [M].....	19
7.3.3	SA-3 – Life Cycle Support [M] .....	19
7.3.4	SA-4 – Acquisitions [M] .....	19
7.3.5	SA-5 – System Documentation [M] .....	20
7.3.6	SA-6 – Software Usage Restrictions [M] .....	21
7.3.7	SA-7 – User-Installed Software [M] .....	21
7.3.8	SA-8 – Security Engineering Principles [M].....	21
7.3.9	SA-9 – External System Services [M] .....	21
7.3.10	SA-10 – Developer Configuration Mgmt [M].....	22
7.3.11	SA-11 – Developer Security Testing [M] .....	22
7.4	Security Assessment and Authorization (CA) Family .....	22
7.4.1	CA-1 – Security Assessment and Authorization P&P [M].....	23
7.4.2	CA-2 – Security Assessments [M] .....	23
7.4.3	CA-3 – Information System Connections [M] .....	23
7.4.4	CA-5 – Plan of Action and Milestones [M].....	24
7.4.5	CA-6 – Security Authorization [M] .....	24
7.4.6	CA-7 – Continuous Monitoring [M] .....	24
7.5	Information Security Program Management (PM) Family.....	25
7.5.1	PM-1 Information Security Program Plan.....	25
7.5.2	PM-2 Senior Information Security Officer.....	25
7.5.3	PM-3 Information Security Resources.....	26
7.5.4	PM-4 Plan Of Action And Milestones Process .....	26
7.5.5	PM-5 Information System Inventory .....	26
7.5.6	PM-6 Info. Security Measures of Performance.....	26
7.5.7	PM-7 Enterprise Architecture .....	26
7.5.8	PM-8 Critical Infrastructure Plan .....	26
7.5.9	PM-9 Risk Management Strategy .....	26
7.5.10	PM-10 Security Authorization Process.....	27
7.5.11	PM-11 Mission/Business Process Definition .....	27
7.6	Identification and Authentication (IA).....	27
7.6.1	IA-1 – Identification& Authentication P&P [M] .....	27
7.6.2	IA-2 – Identification and Authentication (Org. Users) [M] .....	28
7.6.3	IA-3 – Device Identification and Authentication [M] .....	28

[sysname] Security Plan

7.6.4	IA-4 – Identifier Management [M]	28
7.6.5	IA-5 – Authenticator Management [M]	29
7.6.6	IA-6 – Authenticator Feedback [M]	30
7.6.7	IA-7 – Cryptographic Module Authent. [M]	30
7.6.8	IA-8 – Identification and Authentication (Non-Organizational Users) [M]	30
7.7	AC – Access Control	30
7.7.1	AC-1 – Access Control P&P [M]	30
7.7.2	AC-2 – Account Management [M]	31
7.7.3	AC-3 – Access Enforcement [M]	32
7.7.4	AC-4 – Information Flow Enforcement [M]	32
7.7.5	AC-5 – Separation of Duties [M]	32
7.7.6	AC-6 – Least Privilege [M]	32
7.7.7	AC-7 – Unsuccessful Login Attempts [M]	33
7.7.8	AC-8 – System Use Notification [M]	33
7.7.9	AC-10 – Concurrent Session Control [M]	34
7.7.10	AC-11 – Session Lock [M]	34
7.7.11	AC-14 – Permitted Actions without Identification or Authentication [M]	34
7.7.12	AC-17 – Remote Access [M]	34
7.7.13	AC-18 – Wireless Access [M]	35
7.7.14	AC-19 – Access Control for Mobile Devices [M]	36
7.7.15	AC-20 – Use of External Info. Systems [M]	36
7.7.16	AC-22 – Publicly Accessible Content [M]	37
7.8	Audit and Accountability (AU) Family	38
7.8.1	AU-1 – Audit and Accountability P&P [M]	38
7.8.2	AU-2 – Auditable Events [M]	38
7.8.3	AU-3 – Content of Audit Records [M]	39
7.8.4	AU-4 – Audit Storage Capacity [M]	39
7.8.5	AU-5 – Response to Audit Failures [M]	39
7.8.6	AU-6 – Audit Review, Analysis, Reporting [M]	40
7.8.7	AU-7 – Audit Reduction and Report Generation [M]	40
7.8.8	AU-8 – Time Stamps [M]	40
7.8.9	AU-9 – Protection of Audit Information [M]	40
7.8.10	AU-10 – Non-Repudiation [M]	40
7.8.11	AU-11 – Audit Record Retention [M]	41
7.8.12	AU-12 – Audit Generation [M]	41
7.9	System and Communications Protection (SC) Family	42
7.9.1	SC-1 – System and Communications Protection P&P [M]	42
7.9.2	SC-2 – Application Partitioning [M]	42
7.9.3	SC-4 – Information in Shared Resources [M]	42
7.9.4	SC-5 – Denial of Service Protection [M]	42
7.9.5	SC-7 – Boundary Protection [M]	42
7.9.6	SC-8 – Transmission Integrity [M]	43
7.9.7	SC-9 – Transmission Confidentiality [M]	43
7.9.8	SC-10 – Network Disconnect [M]	44
7.9.9	SC-12 – Cryptographic Key Establishment and Management [M]	44
7.9.10	SC-13 – Use of Cryptography [M]	44
7.9.11	SC-14 – Public Access Protections [M]	44

[sysname] Security Plan

7.9.12	SC-15 – Collaborative Computing Devices [M]	44
7.9.13	SC-17 – Public Key Infrastructure Certs [M]	45
7.9.14	SC-18 – Mobile Code [M]	45
7.9.15	SC-19 – Voice Over Internet Protocol [M]	45
7.9.16	SC-20 – Secure Name Resource Svc. (Auth Source) [M]	45
7.9.17	SC-22 – Architecture for Name Res. Svc. [M]	46
7.9.18	SC-23 – Session Authenticity [M]	46
7.9.19	SC-28 – Protection of Information at Rest [M]	46
7.9.20	SC-32 – Information System Partitioning [M]	46
7.9.21	SC-ACA-1 – Electronic Mail [M]-1 – Electronic Mail [M]	46
7.10	Personnel Security (PS) Family	46
7.10.1	PS-1 – Personnel Security P&P [M]	46
7.10.2	PS-2 – Position Categorization [M]	47
7.10.3	PS-3 – Personnel Screening [M]	47
7.10.4	PS-4 – Personnel Termination [M]	47
7.10.5	PS-5 – Personnel Transfer [M]	47
7.10.6	PS-6 – Access Agreements [M]	48
7.10.7	PS-7 – Third-Party Personnel Security [M]	48
7.10.8	PS-8 – Personnel Sanctions [M]	48
7.11	Physical and Environmental Protection (PE) Family	48
7.11.1	PE-1 – Physical and Envir. Protection P&P [M]	48
7.11.2	PE-2 – Physical Access Authorizations [M]	49
7.11.3	PE-3 – Physical Access Control [M]	49
7.11.4	PE-4 – Access Control for Transmission Medium [M]	50
7.11.5	PE-5 – Access Control for Output Devices [M]	50
7.11.6	PE-6 – Monitoring Physical Access [M]	50
7.11.7	PE-7 – Visitor Control [M]	50
7.11.8	PE-8 – Access Records [M]	50
7.11.9	PE-9 – Power Equipment and Cabling [M]	51
7.11.10	PE-10 – Emergency Shutoff [M]	51
7.11.11	PE-11 – Emergency Power [M]	51
7.11.12	PE-12 – Emergency Lighting [M]	51
7.11.13	PE-13 – Fire Protection [M]	51
7.11.14	PE-14 – Temp. and Humidity Controls [M]	52
7.11.15	PE-15 – Water Damage Protection [M]	52
7.11.16	PE-16 – Delivery and Removal [M]	52
7.11.17	PE-17 – Alternate Work Site [M]	52
7.11.18	PE-18 – Location of System Components [M]	53
7.12	Contingency Planning (CP) Family	53
7.12.1	CP-1 – Contingency Planning P&P [M]	53
7.12.2	CP-2 – Contingency Plan [M]	53
7.12.3	CP-3 – Contingency Training [M]	54
7.12.4	CP-4 – Contingency Testing and Exercises [M]	54
7.12.5	CP-6 – Alternate Storage Site [M]	54
7.12.6	CP-7 – Alternate Processing Site [M]	54
7.12.7	CP-8 – Telecommunications Services [M]	55
7.12.8	CP-9 – Information System Backup [M]	55

[sysname] Security Plan

7.12.9	CP-10 – Information System Recovery [M]	56
7.13	Configuration Management (CM)	56
7.13.1	CM-1 – Configuration Management P&P [M]	56
7.13.2	CM-2 – Baseline Configuration [M]	56
7.13.3	CM-3 – Configuration Change Control [M]	57
7.13.4	CM-4 – Security Impact Analysis [M]	57
7.13.5	CM-5 – Access Restrictions for Change [M]	57
7.13.6	CM-6 – Configuration Settings [M]	58
7.13.7	CM-7 – Least Functionality [M]	58
7.13.8	CM-8 – System Component Inventory [M]	58
7.13.9	CM-9 – Configuration Management Plan [M]	59
7.14	Maintenance (MA) Family	59
7.14.1	MA-1 – System Maintenance P&P [M]	59
7.14.2	MA-2 – Controlled Maintenance [M]	59
7.14.3	MA-3 – Maintenance Tools [M]	60
7.14.4	MA-4 – Non-Local Maintenance [M]	60
7.14.5	MA-5 – Maintenance Personnel [M]	61
7.14.6	MA-6 – Timely Maintenance [M]	61
7.15	System and Information Integrity (SI)	61
7.15.1	SI-1 – System and Info Integrity P&P [M]	61
7.15.2	SI-2 – Flaw Remediation [M]	62
7.15.3	SI-3 – Malicious Code Protection [M]	62
7.15.4	SI-4 – Information System Monitoring [M]	63
7.15.5	SI-5 – Security Alerts, Advisories, and Directives [M]	64
7.15.6	SI-7 – Software and Information Integrity [M]	64
7.15.7	SI-8 – Spam Protection [M]	64
7.15.8	SI-9 – Information Input Restrictions [M]	65
7.15.9	SI-10 – Information Input Validation [M]	65
7.15.10	SI-11 – Error Handling [M]	65
7.15.11	SI-12 – Information Output Handling and Retention [M]	65
7.16	Media Protection (MP) Family	65
7.16.1	MP-1 – Media Protection P&P [M]	65
7.16.2	MP-2 – Media Access [M]	66
7.16.3	MP-3 – Media Marking [M]	66
7.16.4	MP-4 – Media Storage [M]	66
7.16.5	MP-5 – Media Transport [M]	66
7.16.6	MP-6 – Media Sanitization [M]	67
7.16.7	MP-ACA-1 – Media Related Records [M]	67
7.17	Incident Response (IR) Family	68
7.17.1	IR-1 – Incident Response P&P [M]	68
7.17.2	IR-2 – Incident Response Training [M]	68
7.17.3	IR-3 – Incident Response Exercises [M]	68
7.17.4	IR-4 – Incident Handling [M]	68
7.17.5	IR-5 – Incident Monitoring [M]	68
7.17.6	IR-6 – Incident Reporting [M]	69
7.17.7	IR-7 – Incident Response Assistance [M]	69
7.17.8	IR-8 – Incident Response Plan [M]	69



**[sysname] Security Plan**

7.18 Awareness and Training (AT) Family .....	70
7.18.1 AT-1 – Security Awareness Training P&P [M].....	70
7.18.2 AT-2 – Security Awareness [M].....	70
7.18.3 AT-3 – Security Training [M].....	71
7.18.4 AT-4 – Security Training Records [M] .....	71
Appendix A – Vendor documentation .....	72
Appendix B – Contracts, etc. ....	72
Appendix C – Acronyms and Abbreviations.....	72

**[sysname] Security Plan**

## 1 Purpose of Document

This document is based on the NIST 800-53 information security and compliance framework. When completed and kept up to date, it helps satisfy many compliance requirements and business needs. For instance, it documents who is responsible for what, what risk DHSS is assuming, how we are mitigating that risk, and how we are ensuring that the documented system or application will have the confidentiality, integrity, and availability you need to help you get your job done.

## 2 Contact Information

<b>2.1 System Name</b>	<b>2.2 Responsible Organization</b>	<b>2.3 System Owner</b>
SOA DHSS [DIV SEC] – [System Name]	DHSS [DIV SEC PRG]	Name: Title: Division Director Phone: (907) Email:
<b>2.4 System Owner Designee</b>	<b>2.5 Program Manager</b>	<b>2.6 Program Manager</b>
Name: Title: Phone: (907) Email:	Name: Title: Phone: (907) Email:	Name: Title: Phone: (907) Email:
<b>2.7 Security Plan Document Owner</b>	<b>2.8 Security Designee</b>	<b>2.9 Vendor Contact</b>
Name: Title: Phone: (907) Email:	Name: Title: Phone: (907) Email:	Name: Title: Phone: (907) Email:
<b>2.10 Primary Technical Contact</b>	<b>2.11 Other Contacts</b>	<b>2.12 Other Contacts</b>
Name: Title: Phone: (907) Email:	Name: Title: Phone: (907) Email:	Name: Title: Phone: (907) Email:



## 3 Information Classification

### 3.1 System Categorization

<input type="checkbox"/>	LOW	<input type="checkbox"/>	MEDIUM	<input type="checkbox"/>	HIGH
--------------------------	-----	--------------------------	--------	--------------------------	------

### 3.2 Data Classification

<input type="checkbox"/>	Public	<input type="checkbox"/>	DHSS Internal Only	<input type="checkbox"/>	DHSS Confidential	<input type="checkbox"/>	DHSS Restricted
<input type="checkbox"/>	PII – Personally Identifiable Information	<input type="checkbox"/>	EPHI – Electronic Protected Health Information (HIPAA)	<input type="checkbox"/>	CJIS – Criminal Justice Information	<input type="checkbox"/>	FERPA
<input type="checkbox"/>	PI/APIPA – Personal Information (APIPA)	<input type="checkbox"/>	PCI / Credit Card info	<input type="checkbox"/>	FTI – Federal Tax Information (IRS PUB 1075)	<input type="checkbox"/>	SAMSHA

### 3.3 Laws, Statutes, & Regulations Governing Information

<input checked="" type="checkbox"/>	Alaska Statutes	<input checked="" type="checkbox"/>	DHSS Policies	<input type="checkbox"/>	HIPAA/HITECH (EPIH)	<input type="checkbox"/>	CJIS Security Policy
<input checked="" type="checkbox"/>	Federal Statutes	<input checked="" type="checkbox"/>	SoA Policies	<input type="checkbox"/>	IRS PUB 1075 (FTI)	<input type="checkbox"/>	PCI DSS
				<input type="checkbox"/>	CMS MARS-E	<input type="checkbox"/>	Other

### 3.4 Agreements with other parties (Business)

Attach all signed contracts MOU/MOAs or BAAs or other agreements with other organizations, partners, vendors, grantees, business associates, or any external parties which affect or are affected by this system as an appendix. List them here:

Organization	Date signed

## 4 Description of System

### 4.1 *The function or purpose of the system and the information processed. (Business)*

*A business description of why the system is needed and what the system is supposed to do:*

### 4.2 *Business process description and diagram (Business)*

### 4.3 *List organizations which use data and how they use it. (Business)*

Sample table:

User organizations	Type of data	Data Use

### 4.4 *System IT Environment (IT)*

- *Include any security measures protecting the system and information.*

### 4.5 *Network Diagrams (IT-NS)*

This section includes the following network diagrams:

[sysname] Security Plan

#### 4.6 List of all linked or dependent applications (IT-BA)

Sample table:

	Type of data	Processing provided	

##### 4.6.1 Referenced Enterprise Services

Sample table (Active Directory, ANC or JNU Data Center, etc...):

DHSS System	Security Plan

#### 4.7 List of Servers and IP addresses (IT-NS)

Server	IP Address	DNS

#### 4.8 List of IP Subnets, Routers, Firewalls (IT-NS)

Device	IP Address	DNS
	.	.

#### 4.9 List of Databases (IT-BA)

[sysname] Security Plan

Database	Server	
	•	•

#### 4.10 System Operational Status

If more than one status is selected, list which part of the system is covered under each status.

- Operational –
- Under Development –

#### 4.11 System Vulnerability Scans and Continuous Monitoring

The most recent vulnerability scan date & continuous monitoring details

Date of scan	Scanning System Used	Highs & Mediums Remediated?

#### 4.12 Patching and Support

Maintenance Windows:

Application/OS	Patching Responsibility	Licensing & Maintenance

#### 4.13 Software Development Environments

System	Development Environment	Data Classification
--------	-------------------------	---------------------


#### **4.14 Information Sensitivity**

### **5 Risk Assessment**

#### **5.1 Information Sensitivity**

#### **5.2 Risk Analysis**

#### **5.3 Risk Assumption**

### **6 Contingency Planning**

#### **6.1 Continuity of Operations Plan (COOP)**

#### **6.2 Disaster Recovery (IT)**

*How is the system going to be returned to operational status for normal State of Alaska DHSS business processes to continue?*

##### **6.2.1 Backups (IT-NS)**

##### **6.2.2 Other Recovery processes**

- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?
- Restriction/controls on those who perform maintenance and repair activities.
- Special procedures for performance of emergency repair and maintenance.
- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.





## 7 NIST 800-53+ Moderate System Controls

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

Status (column D)	
Implemented	I
Inherited	In
Compensated	C
Not Applicable	N
Planned	P
Planned Delayed	PD

Abbr.	Responsible Now

SN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
1.	800000	RA-00	<b>7.1 Risk Assessment (RA) Family</b>				
2.	800000	RA-01	<b>7.1.1 RA-1 – Risk Assessment P&amp;P [M]</b> [NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]				
3.	800001	RA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P	The Department Security Office (DSO) will review/update Risk Assessment policies annually.	
4.	800002	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	The following policies exist around Risk Assessment: ISP-102: Risk Management; ISPGI-122: Guidelines Protection of Personally Identifiable Information; ISP-123: Security Categorization of Information and Information Systems; ISP-173: Network Security; ISP-193: Vulnerability and Patch Management; ISP-201: IS Continuity of Operations; 727: Information Security Framework; 752: Vulnerability Management; 753: Continuity of Operations	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
5.	500001	RA-01b	b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	L	P	The Data Owner, _____, in collaboration with the DSO, will develop formal, documented procedures for Risk Assessment, and will review them annually.	
6.	500200	RA-02	<b>7.1.2 RA-2 – Security Categorization [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
7.	500201	RA-02a	The organization shall: a. Categorize information and the information system in accordance with applicable federal standards and guidance.	M		This security plan is the procedure for meeting this requirement.	
8.	500202	RA-02b	b. Document the security categorization results (including supporting rationale) in the security plan for the information system.	M		This security plan is the procedure for meeting this requirement.	
9.	500203	RA-02c	c. Ensure the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	M		The review and approval phase will be conducted	
10.	500300	RA-03	<b>7.1.3 RA-3 – Risk Assessment [M]</b> [NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]				
11.	500301	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		This security plan is part of the assessment of risk. In addition, a vulnerability scan will be performed. A static code scan will be performed, if required by the Department Security Office.	
12.	500302	RA-03b	b. Document risk assessment results.	M		This security plan is part of the risk assessment results.	
13.	500303	RA-03c	c. Review risk assessment results within every three-hundred-sixty-five (365) days.	M		The DSO and data owner, _____, are responsible for this.	
14.	500304	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		The data owner is responsible for this.	
15.	500305	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			
16.	500306	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		This security plan is the procedure for meeting this requirement.	
17.	500400	RA-05	<b>7.1.4 RA-5 – Vulnerability Scanning [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
18.	810401	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		<coordinate schedule with the DSO, then document schedule here>	
19.	810402	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		DHSS has standard, enterprise tools and techniques that meet these requirements. These tools and techniques change as needed to accommodate an ever changing information technology environment. The DSO can provide a list of current tools/techniques upon request.	
20.	810403	RA-05c	c. Analyze vulnerability scan reports and results from security control assessments.	M		The DSO does this.	
21.	810404	RA-05d	d. Remediate legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk.	M		The DSO assigns and tracks remediation, as needed, to applicable DHSS and DOA IT staff, contractors, grantees, vendors, and other business partners.	
22.	810405	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		The DSO evaluates scan results and acts as needed to eliminate similar vulnerabilities in other information systems.	
23.	810406	RA-05f	f. Employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	M		Our scanning tools include this capability.	
24.	819900	RA-99	This line is a blank spacer line.				
25.	820000	PL-00	<b>7.2 Planning (PL) Family</b>				
26.	820100	PL-01	<b>7.2.1 PL-1 – Security Planning P&amp;P [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
27.	820101	PL-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P	The Department Security Office (DSO) will review/update Planning policies and procedures annually.	
28.	820102	PL-01a	a. A formal, documented security planning <b>policy</b> that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	I	The following policies exist around Planning: ISP-162: System Planning and Acceptance; ISP-163: Electronic Messaging and Archiving; ISP-172: Business Use/Acceptable Use; ISP-211: Copyright Information and Software Licensing; 727: Information Security Framework; 738: Portable Media and Devices; 741: System Planning and Acceptance; 742: Electronic Messaging	
29.	820103	PL-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the security planning policy and associated security planning controls.	L	P	The DSO will develop formal, documented procedures to facilitate the implementation of security planning policy and associated security planning controls, and will review them annually.	
30.	820200	PL-02	<b>7.2.2 PL-2 – System Security Plan (SSP) [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
31.	820201	PL-02a	The organization shall: a. <b>Develop a security plan for the information system</b> that: i. Is consistent with the <b>ACA System Security Plan (SSP) Procedure</b> . ii. Is consistent with the State's enterprise architecture. iii. Explicitly defines the authorization boundary for the system. iv. Describes the operational context of the system in terms of missions and business processes. v. Describes the operational environment for the system. vi. Describes relationships with or connections to other information systems. vii. Provides an overview of the security requirements for the system. viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions. ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.	M		This security plan satisfies i-viii of this requirement. ix is satisfied by the authorization process that occurs after	
32.	820202	PL-02b	b. Review the security plan for the information system within every three-hundred-sixty-five (365) days.	M		The data owner data owner, _____, is responsible for this.	
33.	820203	PL-02c	c. Update the plan, minimally every three (3) years, to address current conditions or whenever: i. There are significant changes to the system/environment of operation that affect security. ii. Problems are identified during plan implementation or security control assessments. iii. When the data sensitivity level increases. iv. After a serious security violation due to changes in the threat environment. v. Before the previous security authorization expires.	M		The data owner data owner, _____, is responsible for this.	
34.	820300	PL-04	<b>7.2.3 PL-4 – Rules of Behavior (ROB) [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
35.	820301	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			
36.	820302	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			
37.	820303	PL-04c	c. <b>[IRS 1075]</b> 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			
38.	820400	PL-05	<b>7.2.4 PL-5 – Privacy Impact Assessment (PIA) [M]</b> [NIST 800-53, CMS MARS-E]				
39.	820401	PL-05a	a. The organization shall conduct a Privacy Impact Assessment (PIA) in accordance with OMB policy M-03-22.	M			
40.	820500	PL-06	<b>7.2.5 PL-6 – Security-Related Activity Planning [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
41.	020001	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		Security related activities will be coordinated through the Security Designee for this system, _____.	
42.	029900	PL-99	This is a blank formatting row.				
43.	030000	SA-00	<b>7.3 System and Services Acquisition (SA)</b>				
44.	030100	SA-01	<b>7.3.1 SA-1 – System&amp; Services Acquisition P&amp;P [M]</b> [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	This is a State and Department requirement. This is not addressed at the system level.	
46.	030102	SA-01a	a. A formal, documented system and services acquisition <b>policy</b> that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	I	This is a State and Department requirement. This is not addressed at the system level.	
47.	030103	SA-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	L	P	This is a State and Department requirement. This is not addressed at the system level.	
48.	030200	SA-02	<b>7.3.2 SA-2 – Allocation of Resources [M]</b> [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		This security plan is designed to provide documentation of the security requirements of this system.	
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		The data owner, _____, is required to determine, document, and request, but not allocate. This is because we are part of the executive branch, which cannot authorize spending for capital projects. Authorization of capital projects is the province of the legislative branch.	
51.	030203	SA-02c	c. Include information security requirements in mission/business case planning.	M		The data owner, _____, is responsible for this.	
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		The data owner, _____, is responsible for this.	
53.	030300	SA-03	<b>7.3.3 SA-3 – Life Cycle Support [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
54.	030301	SA-03a	The organization shall: a. Manage the lifecycle of the information system.	M		<insert here a description of	
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	<b>7.3.4 SA-4 – Acquisitions [M]</b> [NIST 800-53, CMS MARS-E]				

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
58.	ES0401	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: <ul style="list-style-type: none"> <li>i. Security functional requirements/specifications.</li> <li>ii. Security-related documentation requirements.</li> <li>iii. Developmental and evaluation-related assurance requirements.</li> </ul>	M			
59.	ES0402	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.	ES0403	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.	ES0404	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.	ES0405	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.	ES0500	SA-05	<b>7.3.5 SA-5 – System Documentation [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
64.	ES0501	SA-05a	The organization shall: <ul style="list-style-type: none"> <li>a. Obtain, protect as required, and make available to authorized personnel, administrator documentation for the information system that describes: <ul style="list-style-type: none"> <li>i. Secure configuration, installation, and operation of the information system.</li> <li>ii. Effective use and maintenance of security features/functions.</li> <li>iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.</li> </ul> </li> </ul>	M		•	
65.	ES0502	SA-05b	b. Obtain, protect as required, and make available to authorized personnel, user documentation for the information system that describes: <ul style="list-style-type: none"> <li>i. User-accessible security features/functions and how to effectively use those security features/functions.</li> <li>ii. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner.</li> <li>iii. User responsibilities in maintaining the security of the information and information system.</li> </ul>	M		•	
66.	ES0503	SA-05c	c. Document attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	M		a.	



[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
67.	SA0504	SA-05d	d. Obtain, protect as required, and make available to authorized personnel, vendor/manufacture 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.	SA0505	SA-05e	e. Obtain, protect as required, and make available to authorized personnel, vendor/manufacture 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.	SA0600	SA-06	<b>7.3.6 SA-6 – Software Usage Restrictions [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
70.	SA0601	SA-06a	The organization shall: a. Use software and associated documentation in accordance with contract agreements and copyright laws.	M		a.	
71.	SA0602	SA-06b	b. Employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.	M		b.	
72.	SA0603	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.	SA0700	SA-07	<b>7.3.7 SA-7 – User-Installed Software [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
74.	SA0701	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.	SA0800	SA-08	<b>7.3.8 SA-8 – Security Engineering Principles [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
76.	SA0801	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.	SA0900	SA-09	<b>7.3.9 SA-9 – External System Services [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, SSA System Security Guidelines]</i>				
78.	SA0901	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.	SA0902	SA-09b	b. Define and document oversight and user roles and responsibilities with regard to external information system services.	M			

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
80.	800903	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.	800904	SA-09d	d. Monitor security control compliance by external service providers.	M			
82.	800905	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.	800906	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.	800907	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.	811000	SA-10	<b>7.3.10 SA-10 – Developer Configuration Mgmt [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
86.	811001	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.	811002	SA-10b	b. Manage and control changes to the information system.	M		b.	
88.	811003	SA-10c	c. Implement only organization-approved changes.	M		c.	
89.	811004	SA-10d	d. Document approved changes to the information system.	M		d.	
90.	811005	SA-10e	e. Track security flaws and flaw resolution.	M		e.	
91.	811100	SA-11	<b>7.3.11 SA-11 – Developer Security Testing [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
92.	811101	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.	811102	SA-11b	b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process.	M			
94.	811103	SA-11c	c. Document the results of the security control assessment and flaw remediation processes.	M		i.	
95.	811104	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.	820900	SA-99	This line is a blank spacer line.				
97.	840000	CA-00	<b>7.4 Security Assessment and Authorization (CA) Family</b>				

[sysname] Security Plan

IN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
98.	940100	CA-01	<b>7.4.1 CA-1 – Security Assessment and Authorization P&amp;P [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
99.	940101	CA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
100.	940102	CA-01a	a. Formal, documented security assessment and authorization <b>policies</b> that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	At the department level, this is the responsibility of the Department Security Office.	
101.	940103	CA-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	L	P	At the department level, this is the responsibility of the Department Security Office, in collaboration with DHSS/FMS/ITS.	
102.	940200	CA-02	<b>7.4.2 CA-2 – Security Assessments [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
103.	940201	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.	940202	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.	940203	CA-02c	c. Produce a security assessment report that documents the results of the assessment.	M		b.	
106.	940204	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.	940205	CA-02e	e. Employ an independent assessor or assessment team to conduct an assessment of the security controls.	M		d.	
108.	940300	CA-03	<b>7.4.3 CA-3 – Information System Connections [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
109.	940301	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.	
110.	940302	CA-03b	b. Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.	M		b.	
111.	940303	CA-03c	c. Monitor the information system connections on an ongoing basis verifying enforcement of security requirements.	M		c.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
112.		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.		CA-05	<b>7.4.4 CA-5 – Plan of Action and Milestones [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
114.		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.		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.		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.		CA-06	<b>7.4.5 CA-6 – Security Authorization [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				
118.		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.		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.		CA-07	<b>7.4.6 CA-7 – Continuous Monitoring [M]</b> [NIST 800-53, The Patient Protection and Affordable Care Act, CMS MARS-E, IRS 1075]				
121.		CA-07a	a. The organization shall establish a continuous monitoring strategy and implement a continuous monitoring program that includes:	M		a.	
122.		CA-07a1	i. A configuration management process for the information system and its constituent components.	M		i.	
123.		CA-07a2	ii. A determination of the security impact of changes to the information system and environment of operation.	M		ii.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
124.	840004	CA-07a3	iii. Ongoing security control assessments in accordance with the <b>organizational continuous monitoring strategy</b> .	M		iii.	
125.	840005	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.	840006	CA-07.1	<b>The use of independent security assessment agents or teams to monitor security controls is not required.</b> 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.	840007	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.	840008	CA-99	This is a blank formatting row.				
129.	850000	PM-00	<b>7.5 Information Security Program Management (PM) Family</b>				
130.	850000	PM-01	<b>7.5.1 PM-1 Information Security Program Plan</b> [NIST 800-53, CMS MARS-E]				
131.	850001	PM-01a	The organization shall: a. Develop and disseminate an organization-wide information <b>security program plan</b> 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		The Department Security Office is the organization-wide information security program. The plan for this program includes the 700 series DHSS policies (see Policy 727 in particular), ITS standard operating procedures, and practices.	
132.	850002	PM-01b	b. Review the organization-wide information security program plan at an organization defined frequency.	M		This is the responsibility of the Department Security Office.	
133.	850003	PM-01c	c. Revise the plan to address organizational changes and problems identified during plan implementation or security control assessments.	M		This is recommended by the Department Security Office.	
134.	850000	PM-02	<b>7.5.2 PM-2 Senior Information Security Officer</b> [NIST 800-53, CMS MARS-E]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
135.		PM-02a	a. The organization shall appoint a senior information security officer with the mission and <b>resources</b> to coordinate, develop, implement, and maintain an organization-wide information security program.	M		DHSS executive leadership is responsible for this.	
136.		PM-03	<b>7.5.3 PM-3 Information Security Resources</b> [NIST 800-53, CMS MARS-E]				
137.		PM-03a	The organization shall: a. <b>Ensure that all capital planning and investment requests include the resources needed to implement the information security program</b> and document all exceptions to this requirement.	M		DHSS executive leadership is responsible for this.	
138.		PM-03b	b. Employ a business case/Exhibit 300/Exhibit 53 to record the resources required.	M		DHSS executive leadership is responsible for this.	
139.		PM-03c	c. Ensure that information security resources are available for expenditure as planned.	M		DHSS executive leadership is responsible for this.	
140.		PM-04	<b>7.5.4 PM-4 Plan Of Action And Milestones Process</b> [NIST 800-53, CMS MARS-E]				
141.		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			
142.		PM-05	<b>7.5.5 PM-5 Information System Inventory</b> [NIST 800-53, CMS MARS-E]				
143.		PM-05a	a. The organization shall develop and maintain an inventory of its information systems.	M		This is the responsibility of all DHSS property managers.	
144.		PM-06	<b>7.5.6 PM-6 Info. Security Measures of Performance</b> [NIST 800-53, CMS MARS-E]				
145.		PM-06a	a. The organization shall develop, monitor, and report on the results of information security measures of performance.	M		a.	
146.		PM-07	<b>7.5.7 PM-7 Enterprise Architecture</b> [NIST 800-53, CMS MARS-E]				
147.		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		The DHSS Security Architect, who reports to the DHSS Chief Security Officer, makes recommendations to executive leadership to accomplish this requirement. It is the responsibility of executive leadership to ensure this is accomplished.	
148.		PM-08	<b>7.5.8 PM-8 Critical Infrastructure Plan</b> [NIST 800-53, CMS MARS-E]				
149.		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		This security plan is a key part of the process to meet this requirement. The IT governance process, which includes security requirements and estimates, is another method to help meet this requirement.	
150.		PM-09	<b>7.5.9 PM-9 Risk Management Strategy</b> [NIST 800-53, CMS MARS-E]				



[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
151.	000001	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. The information security plan and program, the risk management process, and our IT Governance process help meet this requirement.	
152.	000002	PM-09b	b. Implement that strategy consistently across the organization.	M		b. No part of the organization is exempt from the information security plan and program, the risk management process, or IT Governance process.	
153.	001000	PM-10	<b>7.5.10 PM-10 Security Authorization Process</b>				
154.	001001	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.	001002	PM-10b	b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and	M		b.	
156.	001003	PM-10c	c. Fully integrates the security authorization processes into an organization-wide risk management program.	M		c.	
157.	001004	PM-10d	<i>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.</i>				
158.	001100	PM-11	<b>7.5.11 PM-11 Mission/Business Process Definition</b>				
159.	001101	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.	001102	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.	001103	PM-11c	<i>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.</i>	M			
162.	009900	PM-99	This is a blank formatting line.				
163.	040000	IA-00	<b>7.6 Identification and Authentication (IA)</b>				
164.	040100	IA-01	<b>7.6.1 IA-1 – Identification&amp; Authentication P&amp;P [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
165.	040101	IA-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
166.	860302	IA-01a	a. A formal, documented identification and authentication <b>policy</b> that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	This is the responsibility of the Department Security Office.	
167.	860303	IA-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	L	P	This is the responsibility of the Department Security Office.	
168.	860300	IA-02	<b>7.6.2 IA-2 – Identification and Authentication (Org. Users) [M]</b> <i>[NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
169.	860301	IA-02a	The information system shall: a. Uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	M		i.	
170.	860302	IA-02b	b. Use <b>multifactor authentication</b> for network access to privileged accounts.	M		a.	
171.	860303	IA-02c	c. Use <b>multifactor authentication</b> for network access to non-privileged accounts.	M		b.	
172.	860304	IA-02d	d. Use <b>multifactor authentication</b> for local access to privileged accounts.	M		c.	
173.	860305	IA-02e	e. Use <b>replay resistant authentication mechanisms for network access to privileged accounts</b> .	M		d.	
174.	860306	IA-02f	f. <i>[IRS 1075]</i> 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.	860300	IA-03	<b>7.6.3 IA-3 – Device Identification and Authentication [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E]</i>				
176.	860301	IA-03a	a. The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection.	M		i.	
177.	860400	IA-04	<b>7.6.4 IA-4 – Identifier Management [M]</b> <i>[NIST 800-53, CMS MARS-E]</i>				
178.	860401	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.	860402	IA-04b	b. Selecting an identifier that uniquely identifies an individual or device.	M		b.	
180.	860403	IA-04c	c. Assigning the user identifier to the intended party or the device identifier to the intended device.	M		c.	
181.	860404	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.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
182.		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.		IA-05	<b>7.6.5 IA-5 – Authenticator Management [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]</i>				
184.		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.		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.		IA-05c	<i>[NIST 800-53, CMS MARS-E, IRS 1075]</i> 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. <i>[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.</i> 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.		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			
188.		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.		IA-05f	<i>[IRS 1075]</i> 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.		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.		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.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
192.	860509	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.	860510	IA-05j	j. User account lockout feature shall disable the user account after 3 unsuccessful login attempts.	M		j.	
194.	860511	IA-05k	k. Account lockout duration shall be permanent until an authorized system administrator reinstates the user account.	M		k.	
195.	860512	IA-05l	l. Default vendor passwords shall be changed upon successful installation of the information system product.	M		l.	
196.	860513	IA-05m	m. System initialization (boot) settings shall be password-protected.	M		m.	
197.	860514	IA-05n	n. Clear-text representation of passwords shall be suppressed (blotted out) when entered at the login screen.	M		n.	
198.	860515	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.	860516	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.	860600	IA-06	<b>7.6.6 IA-6 – Authenticator Feedback [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
201.	860601	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.	860700	IA-07	<b>7.6.7 IA-7 – Cryptographic Module Authent. [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
203.	860701	IA-07a	a. The information system shall use mechanisms for <b>authentication to a cryptographic module</b> that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	M		a.	
204.	860800	IA-08	<b>7.6.8 IA-8 – Identification and Authentication (Non-Organizational Users) [M]</b> [NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]				
205.	860801	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.	869900	IA-99	This is a blank formatting line.				
207.	870000	AC-00	<b>7.7 AC – Access Control</b>				
208.	870100	AC-01	<b>7.7.1 AC-1 – Access Control P&amp;P [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				
209.	870101	AC-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
210.	870202	AC-01a	a. A formal, documented access control <b>policy</b> that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
211.	870203	AC-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the access control policy and associated access controls.	L	P		
212.	870209	AC-02	<b>7.7.2 AC-2 – Account Management [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
213.	870205	AC-02a	a. The organization shall manage information system accounts, including:	M			
214.	870202	AC-02a1	i. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary).	M		i.	
215.	870203	AC-02a2	ii. Establishing conditions for group membership.	M		ii.	
216.	870204	AC-02a3	iii. Identifying authorized users of the information system and specifying access privileges.	M		iii.	
217.	870205	AC-02a4	iv. Requiring appropriate approvals for requests to establish accounts.	M		iv.	
218.	870206	AC-02a5	v. Establishing, activating, modifying, disabling, and removing accounts.	M		v.	
219.	870207	AC-02a6	vi. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts.	M		vi.	
220.	870208	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.	870209	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.	870210	AC-02a9	ix. Terminating emergency accounts within twenty-four (24) hours.	M		ix.	
223.	870211	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.	870212	AC-02a11	xi. Reviewing information system accounts within every one-hundred-eighty (180) days and requiring annual certification.	M		xi.	
225.	870213	AC-02a12	xii. Automatically audit account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	M		xii.	
226.	870214	AC-02.1	The organization employs automated mechanisms to support the management of information system accounts.	M			
227.	870215	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.	870216	AC-02.3	The information system automatically disables inactive accounts after one hundred eighty (180) days.	M			
229.	870217	AC-02.4	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	M			

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
230.	[P70218]	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.	[P70219]	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.	[P70220]	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.	[P70300]	AC-03	<b>7.7.3 AC-3 – Access Enforcement [M]</b> <i>[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]</i>				
234.	[P70301]	AC-03a	a. The information system shall enforce approved authorizations for logical access to the system in accordance with applicable policy.	M		i.	
235.	[P70302]	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.	[P70400]	AC-04	<b>7.7.4 AC-4 – Information Flow Enforcement [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
237.	[P70401]	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.	[P70402]	AC-04b	b. <i>[ISO 27001:2005]</i> Groups of information services, users, and information systems shall be segregated on networks.	M		a.	
239.	[P70403]	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.	[P70404]	AC-04d	d. Opportunities for information leakage shall be prevented.	M		c.	
241.	[P70500]	AC-05	<b>7.7.5 AC-5 – Separation of Duties [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
242.	[P70501]	AC-05a	The organization shall: a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.	M		a.	
243.	[P70502]	AC-05b	b. Document separation of duties.	M		b.	
244.	[P70503]	AC-05c	c. Implement separation of duties through assigned information system access authorizations.	M		c.	
245.	[P70600]	AC-06	<b>7.7.6 AC-6 – Least Privilege [M]</b> <i>[NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075, SSA System Security Guidelines]</i>				



[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
246.	870601	AC-06a	The organization shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with system missions and business functions.	M		i.	
247.	870602	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.	870603	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.	870700	AC-07	<b>7.7.7 AC-7 – Unsuccessful Login Attempts [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
250.	870701	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.	870702	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.	870800	AC-08	<b>7.7.8 AC-8 – System Use Notification [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
253.	870801	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: <ul style="list-style-type: none"> <li>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.</li> <li>Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.</li> <li>By using this information system, you understand and consent to the following: <ul style="list-style-type: none"> <li>* 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.</li> <li>* Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.</li> </ul> </li> </ul>	M			
254.	870802	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.	

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
255.	870803	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.	870900	AC-10	<b>7.7.9 AC-10 – Concurrent Session Control [M]</b> <i>[NIST 800-53, CMS MARS-E]</i>				
257.	870901	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.	871000	AC-11	<b>7.7.10 AC-11 – Session Lock [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
259.	871001	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.	871002	AC-11b	b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.	M		a.	
261.	871100	AC-14	<b>7.7.11 AC-14 – Permitted Actions without Identification or Authentication [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
262.	871101	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.	871102	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.	871103	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.	871200	AC-17	<b>7.7.12 AC-17 – Remote Access [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
266.	871201	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.	871202	AC-17a	If authorized, the organization shall: a. Document allowed methods of remote access to the information system.	M		a.	
268.	871203	AC-17b	b. Establish usage restrictions and implementation guidance for each allowed remote access method.	M		b.	

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
269.	871204	AC-17c	c. Monitor for unauthorized remote access to the information system.	M		c.	
270.	871205	AC-17d	d. Authorize remote access to the information system prior to connection.	M		d.	
271.	871206	AC-17e	e. Enforce requirements for remote connections to the information system.	M		e.	
272.	871207	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.	871208	AC-17g	g. The information system shall route all remote accesses through a limited number of managed access control points.	M		g.	
274.	871209	AC-17h	[NIST 800-53] The organization shall: h. Use cryptography to protect the confidentiality and integrity of remote access sessions.	M		h.	
275.	871210	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.	871211	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.	871212	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.	
278.	871213	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.	871214	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.	871300	AC-18	<b>7.7.13 AC-18 – Wireless Access [M]</b> [NIST 800-53, CMS MARS-E]				
281.	871301	AC-18	The organization shall prohibit the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization shall:	M			
282.	871302	AC-18a	a. Monitor for unauthorized wireless access to the information system.	M			
283.	871303	AC-18b	b. Enforce requirements for wireless connections to the information system.	M			
284.	871304	AC-18c	c. Protect wireless access to the system using authentication and encryption if wireless access is explicitly approved.	M			
285.	871305	AC-18d	[NIST 800-53, IRS 1075] The organization shall d. Establish policy, usage restrictions and implementation guidance for wireless access.	M			
286.	871306	AC-18e	e. Authorize wireless access to the information system prior to connection.	M			

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
287.	371400	AC-19	<b>7.7.14 AC-19 – Access Control for Mobile Devices [M]</b> <i>[NIST 800-53, CMS MARS-E]</i>				
288.	371401	AC-19	The organization shall prohibit the connection of portable and mobile devices [e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations] to information systems <b>unless explicitly authorized</b> , in writing, by the CIO or his/her designated representative. <b>If authorized, the organization shall:</b>	M			
289.	371402	AC-19a	a. Monitor for unauthorized connections of mobile devices to information systems.	M			
290.	371403	AC-19b	b. Enforce requirements for the connection of mobile devices to information systems.	M			
291.	371404	AC-19c	c. Disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.	M			
292.	371405	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.	371406	AC-19e	<i>[NIST 800-53, ISO 27001:2005, IRS 1075]</i> e. The organization shall establish a formal policy, usage restrictions and implementation guidance for organization-controlled mobile devices.	M			
294.	371407	AC-19f	<i>[NIST 800-53]</i> The organization shall f. Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems.	M			
295.	371408	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.	371409	AC-19h	h. Restrict the use of writable, removable media in organizational information systems.	M			
297.	371410	AC-19i	i. Prohibit the use of personally owned, removable media in organizational information systems.	M			
298.	371411	AC-19j	j. Prohibit the use of removable media in organizational information systems when the media has no identifiable owner.	M			
299.	371412	AC-19k	<i>[CMS MARS-E]</i> 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.	371413	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.	371500	AC-20	<b>7.7.15 AC-20 – Use of External Info. Systems [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
302.	871301	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.	871302	AC-20a	a. The types of applications that can be accessed from external information systems.	M		a.	
304.	871303	AC-20b	<b>b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted.</b>	M		b. The FIPS 199 security category of information is medium.	
305.	871303	AC-20c	c. How other users of the external information system will be prevented from accessing federal information.	M		c.	
306.	871304	AC-20d	d. The use of virtual private networking (VPN) and firewall technologies.	M		d.	
307.	871305	AC-20e	e. The use of and protection against the vulnerabilities of <b>wireless</b> technologies.	M		e.	
308.	871306	AC-20f	f. The maintenance of adequate physical security controls.	M		f.	
309.	871307	AC-20g	g. The use of virus and spyware protection software.	M		g.	
310.	871308	AC-20h	h. How often the security capabilities of installed software are to be updated.	M		h.	
311.	871309	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.	871310	AC-20.1b	b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system	M			
313.	871511	AC-20.2	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	M			
314.	871800	AC-22	<b>7.7.16 AC-22 – Publicly Accessible Content</b> <b>[M]</b> <i>[NIST 800-53, CMS MARS-E]</i>				
315.	871801	AC-22a	The organization shall: a. Designate individuals authorized to post information onto an organizational information system that is publicly accessible.	M			
316.	871802	AC-22b	b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	M			
317.	871803	AC-22c	c. Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.	M			
318.	871804	AC-22d	d. Review the content on the publicly accessible organizational information system for nonpublic information at an organization-defined frequency.	M			

[sysname] Security Plan

IN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
319.	571405	AC-22e	e. Remove nonpublic information from the publicly accessible organizational information system, if discovered.	M			
320.	580000	AU-00	<b>7.8 Audit and Accountability (AU) Family</b>				
321.	580100	AU-01	<b>7.8.1 AU-1 – Audit and Accountability P&amp;P [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
322.	580101	AU-01	The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days:	L	P		
323.	580102	AU-01a	a. A formal, documented audit and accountability <b>policy</b> that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
324.	580103	AU-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	L	P	b.	
325.	580200	AU-02	<b>7.8.2 AU-2 – Auditable Events [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				
326.	580201	AU-02a	The organization shall: a. Determine, based on a risk assessment and mission/business needs, that <b>the information system must be capable of auditing</b> the following list of auditable events:	M		a.	
327.	580202	AU-02a1	i. Server alerts and error messages.	M			
328.	580203	AU-02a2	ii. User log-on and log-off (successful or unsuccessful).	M			
329.	580204	AU-02a3	iii. All system administration activities.	M			
330.	580205	AU-02a4	iv. Modification of privileges and access.	M			
331.	580206	AU-02a5	v. Start up and shut down.	M			
332.	580207	AU-02a6	vi. Application modifications.	M			
333.	580208	AU-02a7	vii. Application alerts and error messages.	M			
334.	580209		viii. Configuration changes.	M			
335.	580210	AU-02a9	ix. Account creation, modification, or deletion.	M			
336.	580211	AU-02a10	x. File creation and deletion.	M			
337.	580212	AU-02a11	xi. Read access to sensitive information.	M			
338.	580213	AU-02a12	xii. Modification to sensitive information.	M			
339.	580214	AU-02a13	xiii. Printing sensitive information.	M			
340.	580215	AU-02b	b. <b>Coordinate the security audit function with other organizational entities</b> requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.	M		b.	

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
341.	980216	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.	980217	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.	980218	AU-02d1	See above.	M			
344.	980219	AU-02d2	See above.	M			
345.	980220	AU-02d3	See above.	M			
346.	980221	AU-02d4	See above.	M			
347.	980222	AU-02d5	See above.	M			
348.	980223	AU-02d6	See above.	M			
349.	980224	AU-02d7	See above.	M			
350.	980225	AU-02d8	See above.	M			
351.	980226	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.	980227	AU-02f	f. Review and update the list of auditable events at an organization-defined frequency.	M		f.	
353.	980300	AU-03	<b>7.8.3 AU-3 – Content of Audit Records [M]</b> [NIST 800-53, ISO 27001:2005, The Patient Protection and Affordable Care Act, CMS MARS-E, SSA System Security Guidelines]				
354.	980301	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.	980302	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.	980400	AU-04	<b>7.8.4 AU-4 – Audit Storage Capacity [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
357.	980401	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.	980500	AU-05	<b>7.8.5 AU-5 – Response to Audit Failures [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
359.	980501	AU-05a	The information system shall: a. Alert designated organizational officials in the event of an audit processing failure.	M		a.	



[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
360.		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.		AU-06	<b>7.8.6 AU-6 – Audit Review, Analysis, Reporting [M]</b> [NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]				
362.		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.		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.		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			
365.		AU-07	<b>7.8.7 AU-7 – Audit Reduction and Report Generation [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
366.		AU-07a	a. The information system shall provide an audit reduction and report generation capability.	M		a.	
367.		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.		AU-08	<b>7.8.8 AU-8 – Time Stamps [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075, SSA System Security Guidelines]				
369.		AU-08a	a. The information system shall use internal system clocks to generate time stamps for audit records.	M		a.	
370.		AU-08b	b. The information system shall synchronize internal information system clocks daily and at system boot.	M		b.	
371.		AU-09	<b>7.8.9 AU-9 – Protection of Audit Information [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075, SSA System Security Guidelines]				
372.		AU-09a	a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.	M		a.	
373.		AU-10	<b>7.8.10 AU-10 – Non-Repudiation [M]</b> [NIST 800-53, CMS MARS-E]				
374.		AU-10a	a. The information system shall protect against an individual falsely denying having performed a particular action.	M		a.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
375.	081.100	AU-11	<b>7.8.11 AU-11 – Audit Record Retention [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
376.	081.101	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.	081.102	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.	081.103	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.	081.104	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.	081.105	AU-11e	e. Audit file data shall be unalterable (read only) and maintained for a minimum of three (preferably seven) years.	M		e.	
381.	081.200	AU-12	<b>7.8.12 AU-12 – Audit Generation [M]</b> [NIST 800-53, The Patient Protection and Affordable Care Act, CMS MARS-E, HITECH]				
382.	081.201	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.	081.202	AU-12a2	ii. All changes to logical access control authorities (e.g., rights, permissions).	M		ii.	
384.	081.203	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.	081.204	AU-12a4	iv. The audit trail shall capture the enabling or disabling of audit report generation services.	M		iv.	
386.	081.205	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.	081.206	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.	081.207	AU-12c	c. Generate audit records for the list of audited events.	M		b.	
389.	081.208	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.	081.209	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.				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
392.	390000	SC-00	<b>7.9 System and Communications Protection (SC) Family</b>				
393.	390100	SC-01	<b>7.9.1 SC-1 – System and Communications Protection P&amp;P [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
394.	390101	SC-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
395.	390102	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.	390103	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.	390104	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.	
398.	390200	SC-02	<b>7.9.2 SC-2 – Application Partitioning [M]</b> [NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]				
399.	390201	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.	390300	SC-04	<b>7.9.3 SC-4 – Information in Shared Resources [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
401.	390301	SC-04a	a. The information system shall prevent unauthorized and unintended information transfer via shared system resources.	M			
402.	390400	SC-05	<b>7.9.4 SC-5 – Denial of Service Protection [M]</b> [NIST 800-53, CMS MARS-E]				
403.	390401	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 <a href="http://www.sans.org/dosstep">www.sans.org/dosstep</a> . ii. SANS Organization's Roadmap to Defeating DDoS <a href="http://www.sans.org/dosstep/roadmap.php">www.sans.org/dosstep/roadmap.php</a> . iii. NIST CVE List <a href="http://checklists.nist.gov/home.cfm">http://checklists.nist.gov/home.cfm</a> .	M		a.	
404.	390402	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.	390403	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.	390500	SC-07	<b>7.9.5 SC-7 – Boundary Protection [M]</b> [NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
407.		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.		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.		SC-07c	c. Physically allocate publicly accessible information system components to separate sub-networks with separate physical network interfaces.	M		c.	
410.		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.		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.	
412.		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.		SC-08	<b>7.9.6 SC-8 – Transmission Integrity [M]</b> [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.		SC-08a	a. The information system shall protect the integrity of transmitted information.	M			
415.		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.		SC-01	<b>7.9.7 SC-9 – Transmission Confidentiality [M]</b> [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.		SC-09a	a. The information system shall protect the confidentiality of transmitted information.	M			

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
418.	990702	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.	990800	SC-10	<b>7.9.8 SC-10 – Network Disconnect [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
420.	990801	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.	990802	SC-10b	b. Forcibly disconnect inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity.	M		b.	
422.	990900	SC-12	<b>7.9.9 SC-12 – Cryptographic Key Establishment and Management [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
423.	990901	SC-12a	a. When cryptography is required and used within the information system, the organization shall establish and <b>manage cryptographic keys</b> for required cryptography employed within the information system.	M		a.	
424.	990902	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.	991000	SC-13	<b>7.9.10 SC-13 – Use of Cryptography [M]</b> [NIST 800-53, ISO 27001:2005, The Patient Protection and Affordable Care Act, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]				
426.	991001	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.	991002	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.	991003	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.	991004	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.	991100	SC-14	<b>7.9.11 SC-14 – Public Access Protections [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
431.	991101	SC-14a	a. The information system shall protect the integrity and availability of publicly available information and applications.	M			
432.	991200	SC-15	<b>7.9.12 SC-15 – Collaborative Computing Devices [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
433.	991201	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: <ul style="list-style-type: none"> <li>i. Prohibit remote activation of collaborative computing devices.</li> <li>ii. Provide an explicit indication of use to users physically present at the devices.</li> </ul>	M			
434.	991202	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.	991300	SC-17	<b>7.9.13 SC-17 – Public Key Infrastructure Certs [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E]</i>				
436.	991301	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.	991302	SC-17b	b. <i>[IRS 1075]</i> The agency shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	M			
438.	991400	SC-18	<b>7.9.14 SC-18 – Mobile Code [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
439.	991401	SC-18a	The organization shall: <ul style="list-style-type: none"> <li>a. Define acceptable and unacceptable mobile code and mobile code technologies.</li> </ul>	M			
440.	991402	SC-18b	b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.	M			
441.	991403	SC-18c	c. Authorize, monitor, and control the use of mobile code within the information system.	M			
442.	991500	SC-19	<b>7.9.15 SC-19 – Voice Over Internet Protocol [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
443.	991501	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: <ul style="list-style-type: none"> <li>a. Establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously.</li> </ul>	M			
444.	991502	SC-19b	b. Authorize, monitor, and control the use of VoIP within the information system.	M			
445.	991600	SC-20	<b>7.9.16 SC-20 – Secure Name Resource Svc. (Auth Source) [M]</b> <i>[NIST 800-53, CMS MARS-E]</i>				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
446.	801801	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.	801802	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.	801700	SC-22	<b>7.9.17 SC-22 – Architecture for Name Res. Svc. [M]</b> [NIST 800-53, CMS MARS-E]				
449.	801701	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.	801800	SC-23	<b>7.9.18 SC-23 – Session Authenticity [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
451.	801801	SC-23a	a. The information system shall provide mechanisms to protect the authenticity of communications sessions.	M		i.	
452.	801900	SC-28	<b>7.9.19 SC-28 – Protection of Information at Rest [M]</b> [NIST 800-53, CMS MARS-E]				
453.	801901	SC-28a	a. The information system shall protect the confidentiality and integrity of information at rest.	M		a.	
454.	802000	SC-32	<b>7.9.20 SC-32 – Information System Partitioning [M]</b> [NIST 800-53, Medicaid Information Tech Architecture, CMS MARS-E]				
455.	802001	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.	802100	SC-66	<b>7.9.21 SC-ACA-1 – Electronic Mail [M]-1 – Electronic Mail [M]</b>				
457.	802101	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.	899900	SC-99	This is a blank formatting line				
459.	800000	PS-00	<b>7.10 Personnel Security (PS) Family</b>				
460.	800100	PS-01	<b>7.10.1 PS-1 – Personnel Security P&amp;P [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				



[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
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.	
466.	100200	PS-02	<b>7.10.2 PS-2 – Position Categorization [M]</b> [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	<b>7.10.3 PS-3 – Personnel Screening [M]</b> [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	<b>7.10.4 PS-4 – Personnel Termination [M]</b> [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	<b>7.10.5 PS-5 – Personnel Transfer [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
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	<b>7.10.6 PS-6 – Access Agreements [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
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	<b>7.10.7 PS-7 – Third-Party Personnel Security [M]</b> [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	<b>7.10.8 PS-8 – Personnel Sanctions [M]</b> [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	<b>7.11 Physical and Environmental Protection (PE) Family</b>				
496.	110100	PE-01	<b>7.11.1 PE-1 – Physical and Envir. Protection P&amp;P [M]</b> [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.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
499.	110101	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	<b>7.11.2 PE-2 – Physical Access Authorizations [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
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.	
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	<b>7.11.3 PE-3 – Physical Access Control [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
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. <i>[ISO 27001:2005]</i> Physical protection and guidelines for working in secure areas shall be designed and applied.	M		g.	
513.	110309	PE-03i	i. <i>[IRS 1075]</i> 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.	

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
515.	[10400]	PE-04	<b>7.11.4 PE-4 – Access Control for Transmission Medium [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
516.	[10401]	PE-04a	a. The organization shall control physical access to information system distribution and transmission lines within organizational facilities.	M		a.	
517.	[10402]	PE-04b	<i>[IRS 1075]</i> 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.	[10403]	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.	
519.	[10500]	PE-05	<b>7.11.5 PE-5 – Access Control for Output Devices [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
520.	[10501]	PE-05a	a. The organization shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	M			
521.	[10600]	PE-06	<b>7.11.6 PE-6 – Monitoring Physical Access [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
522.	[10601]	PE-06a	The organization shall: a. Monitor physical access to the information system to detect and respond to physical security incidents.	M		a.	
523.	[10602]	PE-06b	b. Review physical access logs at least semi-annually.	M		b.	
524.	[10603]	PE-06c	c. Coordinate results of reviews and investigations with the organization's incident response capability.	M		c.	
525.	[10604]	PE-06d	d. Monitor real-time physical intrusion alarms and surveillance equipment.	M		d.	
526.	[10700]	PE-07	<b>7.11.7 PE-7 – Visitor Control [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
527.	[10701]	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.	[10702]	PE-07b	b. Escort visitors and monitor visitor activity, when required.	M		a.	
529.	[10800]	PE-08	<b>7.11.8 PE-8 – Access Records [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
530.	[10801]	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.	[10802]	PE-08b	b. Review visitor access records monthly.	M		b.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
532.		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.		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.		PE-08e	e. Designated officials or designees within the organization shall review the visitor access records, at least annually.	M		e.	
535.		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.		PE-09	<b>7.11.9 PE-9 – Power Equipment and Cabling [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
537.		PE-09a	a. The organization shall protect power equipment and power cabling for the information system from damage and destruction.	M		a.	
538.		PE-10	<b>7.11.10 PE-10 – Emergency Shutoff [M]</b> [NIST 800-53, CMS MARS-E]				
539.		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.		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.		PE-10c	c. Protect emergency power shutoff capability from unauthorized activation.	M		c.	
542.		PE-11	<b>7.11.11 PE-11 – Emergency Power [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
543.		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.		PE-12	<b>7.11.12 PE-12 – Emergency Lighting [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
545.		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.		PE-13	<b>7.11.13 PE-13 – Fire Protection [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
547.	[11301]	PE-13a	The organization shall: a. Employ and maintain fire suppression and detection devices/systems for the information system.	M		i.	
548.	[11302]	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.	[11303]	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.	
550.	[11304]	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.	[11400]	PE-14	<b>7.11.14 PE-14 – Temp. and Humidity Controls [M]</b> <i>[NIST 800-53, CMS MARS-E]</i>				
552.	[11401]	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.	[11402]	PE-14b	b. Monitor temperature and humidity levels.	M		b.	
554.	[11500]	PE-15	<b>7.11.15 PE-15 – Water Damage Protection [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E]</i>				
555.	[11501]	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.	[11600]	PE-16	<b>7.11.16 PE-16 – Delivery and Removal [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
557.	[11601]	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.	[11700]	PE-17	<b>7.11.17 PE-17 – Alternate Work Site [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E]</i>				
559.	[11701]	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.	[11702]	PE-17b	b. Assess as feasible, the effectiveness of security controls at alternate work sites.	M		b.	
561.	[11703]	PE-17c	c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.	M		c.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
562.		PE-18	<b>7.11.18 PE-18 – Location of System Components [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
563.		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.		PE-99	This is a blank formatting row.				
565.		CP-00	<b>7.12 Contingency Planning (CP) Family</b>				
566.		CP-01	<b>7.12.1 CP-1 – Contingency Planning P&amp;P [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
567.		CP-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
568.		CP-01a	a. A formal, documented contingency planning <b>policy</b> that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
569.		CP-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	L	P	b.	
570.		CP-02	<b>7.12.2 CP-2 – Contingency Plan [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]</i>				
571.		CP-02a	The organization shall: a. Develop a Contingency Plan (CP) for the information system that: i. Identifies essential system missions and business functions and associated contingency requirements. ii. Provides recovery objectives, restoration priorities, and metrics. iii. Addresses contingency roles, responsibilities, assigned individuals with contact information. iv. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure. v. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented. vi. Is reviewed and approved by designated officials within the organization.	M		i.	
572.		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.		CP-02c	c. Coordinate contingency planning activities with incident handling activities.	M		a.	
574.		CP-02d	d. Review the CP for the information system within every three-hundred-sixty-five (365) days.	M			
575.		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.	



[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
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			
579.	120300	CP-03	<b>7.12.3 CP-3 – Contingency Training [M]</b> [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	<b>7.12.4 CP-4 – Contingency Testing and Exercises [M]</b> [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	<b>7.12.5 CP-6 – Alternate Storage Site [M]</b> [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	<b>7.12.6 CP-7 – Alternate Processing Site [M]</b> [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.	

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
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.	
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	<b>7.12.7 CP-8 – Telecommunications Services</b> <b>[M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
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	<b>7.12.8 CP-9 – Information System Backup [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</i>				
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 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. <i>[IRS 1075]</i> 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.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
606.	120900	CP-10	<b>7.12.9 CP-10 – Information System Recovery [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]</i>				
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	<b>7.13 Configuration Management (CM)</b>				
612.	130100	CM-01	<b>7.13.1 CM-1 – Configuration Management P&amp;P [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
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	<b>7.13.2 CM-2 – Baseline Configuration [M]</b> <i>[NIST 80-53, ISO 27001:2005, CMS MARS-E, IRS 1075]</i>				
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.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
622.	E30300	CM-03	<b>7.13.3 CM-3 – Configuration Change Control [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
623.	E30301	CM-03a	The organization shall: a. Determine the types of changes to the information system that are configuration controlled.	M		a.	
624.	E30302	CM-03b	b. Approve configuration-controlled changes to the system with explicit consideration for security impact analyses.	M		b.	
625.	E30303	CM-03c	c. Document approved configuration-controlled changes to the system.	M		c.	
626.	E30304	CM-03d	d. Retain and review records of configuration-controlled changes to the system.	M		d.	
627.	E30305	CM-03e	e. Audit activities associated with configuration-controlled changes to the system.	M		e.	
628.	E30306	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.	E30307	CM-03g	g. Test, validate, and document changes to the information system before implementing the changes on the operational system.	M		f.	
630.	E30400	CM-04	<b>7.13.4 CM-4 – Security Impact Analysis [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
631.	E30401	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.	E30402	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.	E30403	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.	E30404	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.	E30500	CM-05	<b>7.13.5 CM-5 – Access Restrictions for Change [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
636.	E30501	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.	E30502	CM-05a2	Continued from above.				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
638.	E30060	CM-06	<b>7.13.6 CM-6 – Configuration Settings [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
639.	E30061	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 <a href="http://intranet.hhs.gov/it/cybersecurity/policies_by_document_type/index.html#Policy and Standard Waiver">http://intranet.hhs.gov/it/cybersecurity/policies_by_document_type/index.html#Policy and Standard Waiver</a> ), with copies submitted to the Department.	M			
640.	E30062	CM-06b	b. Implement the configuration settings.	M		a.	
641.	E30063	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.	E30064	CM-06d	d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	M		c.	
643.	E30065	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.	E30700	CM-07	<b>7.13.7 CM-7 – Least Functionality [M]</b> [NIST 800-53, Medicaid Information Technology Architecture, CMS MARS-E, IRS 1075]				
645.	E30701	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.	E30702	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.	E30800	CM-08	<b>7.13.8 CM-8 – System Component Inventory [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cntrl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
648.	[330801]	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.	[330802]	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.	[330803]	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.	[330900]	CM-09	<b>7.13.9 CM-9 – Configuration Management Plan [M]</b> [NIST 800-53, CMS MARS-E]				
652.	[330901]	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.	[330902]	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.	[330903]	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.	[339900]	CM-99	Blank formatting line.				
656.	[340000]	MA-00	<b>7.14 Maintenance (MA) Family</b>				
657.	[340100]	MA-01	<b>7.14.1 MA-1 – System Maintenance P&amp;P [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
658.	[340101]	MA-01	The organization shall develop, disseminate, and review/update within every three hundred sixty-five (365) days:	L	P		
659.	[340102]	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.	[340103]	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.	[340200]	MA-02	<b>7.14.2 MA-2 – Controlled Maintenance [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
662.	[S40201]	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.	[S40202]	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.	[S40203]	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.	[S40204]	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.	[S40205]	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.	[S40206]	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.	[S40300]	MA-03	<b>7.14.3 MA-3 – Maintenance Tools [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
669.	[S40301]	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.	[S40302]	MA-03b	b. Inspect all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.	M		b.	
671.	[S40303]	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.	[S40400]	MA-04	<b>7.14.4 MA-4 – Non-Local Maintenance [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
673.	[S40401]	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.	[S40402]	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.	[S40403]	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.	[S40404]	MA-04c	c. Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions.	M		c.	
677.	[S40405]	MA-04d	d. Maintain records for non-local maintenance and diagnostic activities.	M		d.	



[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
678.	[A0406]	MA-04e	e. Terminate all sessions and network connections when non-local maintenance is completed.	M		e.	
679.	[A0407]	MA-04f	f. <b>Not required per CMS – 2014-02-27</b> Audit non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.	M		f.	
680.	[A0408]	MA-04g	g. <b>Not required per CMS – 2014-02-27</b> Document, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	M		g.	
681.	[A0409]	MA-04h	h. <b>Not required per CMS – 2014-02-27</b> 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.	[A0410]	MA-04i	i. <b>NR CMS – 2014-02-27</b> 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.	[A0500]	MA-05	<b>7.14.5 MA-5 – Maintenance Personnel [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				
684.	[A0501]	MA-05a	The organization shall: a. Establish a process for <b>maintenance personnel authorization</b> and maintain a current list of authorized maintenance organizations or personnel.	M		a.	
685.	[A0502]	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.	[A0600]	MA-06	<b>7.14.6 MA-6 – Timely Maintenance [M]</b> [NIST 800-53, CMS MARS-E]				
687.	[A0601]	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.	[A0900]	MA-99	This is a blank formatting row.				
689.	[S0000]	SI-00	<b>7.15 System and Information Integrity (SI)</b>				
690.	[S0100]	SI-01	<b>7.15.1 SI-1 – System and Info Integrity P&amp;P [M]</b> [NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]				
691.	[S0101]	SI-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
692.	ISO 9001	SI-01a	a. A formal, documented system and information integrity <b>policy</b> that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	I	a.	
693.	ISO 9001	SI-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	L	P	b.	
694.	ISO 2000	SI-02	<b>7.15.2 SI-2 – Flaw Remediation [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
695.	ISO 9001	SI-02a	The organization shall: a. Identify, report, and correct information system flaws.	M			
696.	ISO 2001	SI-02b	b. Test software updates related to flaw remediation for effectiveness and potential side effects on information systems before installation.	M			
697.	ISO 2001	SI-02c	c. Incorporate flaw remediation into the organizational configuration management process.	M		c.	
698.	ISO 2004	SI-02d	d. Centrally manage the flaw remediation process and install software updates automatically.	M		d.	
699.	ISO 2005	SI-02e	e. Employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.	M		e.	
700.	ISO 3000	SI-03	<b>7.15.3 SI-3 – Malicious Code Protection [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				
701.	ISO 3001	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.	ISO 3002	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.	ISO 3003	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.	ISO 3004	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.	ISO 3005	SI-03e	e. Centrally manage malicious code protection mechanisms.	M		e.	
706.	ISO 3006	SI-03f	f. Ensure that the information system automatically updates malicious code protection mechanisms (including signature definitions).	M		f.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
707.	ISO307	SI-03g	g. Ensure that the information system prevents non-privileged users from circumventing malicious code protection capabilities.	M		g.	
708.	ISO308	SI-03h	h. [ISO 27001:2005] The organization shall implement appropriate user awareness procedures.	M		h.	
709.	ISO400	SI-04	<b>7.15.4 SI-4 – Information System Monitoring</b> <b>[M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
710.	ISO401	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.	ISO402	SI-04b	b. Identify unauthorized use of the system.	M		b.	
712.	ISO403	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.	ISO404	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.	ISO405	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.	ISO406	SI-04f	f. Interconnect and configure individual intrusion detection tools into a system wide intrusion detection system using common protocols.	M		f.	
716.	ISO407	SI-04g	g. Employ automated tools to support near real-time analysis of events.	M		g.	
717.	ISO408	SI-04h	h. Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.	M		h.	
718.	ISO409	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.	ISO410	SI-04j	j. Ensure that the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	M		i.	

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
720.	[500411]	SI-04k	<p>[SSA System Security Guidelines]</p> <p>k. The system shall produce reports providing management and/or supervisors with the capability to appropriately monitor user activity, such as:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> </ul>	M		i.	
721.	[500500]	SI-05	<p><b>7.15.5 SI-5 – Security Alerts, Advisories, and Directives [M]</b></p> <p>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]</p>				
722.	[500501]	SI-05a	<p>The organization shall:</p> <p>a. Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.</p>	M		a.	
723.	[500502]	SI-05b	<p>b. Generate internal security alerts, advisories, and directives as deemed necessary.</p>	M		b.	
724.	[500503]	SI-05c	<p>c. Disseminate security alerts, advisories, and directives to appropriate personnel.</p>	M		c.	
725.	[500504]	SI-05d	<p>d. Implement security directives in accordance with established time frames, or notifies the degree of noncompliance.</p>	M		d.	
726.	[500600]	SI-07	<p><b>7.15.6 SI-7 – Software and Information Integrity [M]</b></p> <p>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]</p>				
727.	[500601]	SI-07a	<p>a. The information system shall detect unauthorized changes to software and information.</p>	M			
728.	[500602]	SI-07b	<p>b. The organization shall reassess the integrity of software and information by performing daily integrity scans of the information system.</p>	M		a.	
729.	[500603]	SI-07c	<p>c. [ISO 27001:2005] Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.</p>	M		i.	
730.	[500700]	SI-08	<p><b>7.15.7 SI-8 – Spam Protection [M]</b></p> <p>[NIST 800-53, CMS MARS-E]</p>				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
731.	[50701]	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.	[50702]	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.	[50703]	SI-08c	c. Centrally manage spam protection mechanisms.	M			
734.	[50704]	SI-08.1	SI-8(1) – Enhancement [M] Control The organization centrally manages spam protection mechanisms.	M			
735.	[50800]	SI-09	<b>7.15.8 SI-9 – Information Input Restrictions [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
736.	[50801]	SI-09a	a. The organization shall restrict the capability to input information to the information system to authorized personnel.	M		a.	
737.	[50900]	SI-10	<b>7.15.9 SI-10 – Information Input Validation [M]</b> [NIST 800-53, ISO 27001:2005, Medicaid Information Technology Architecture, CMS MARS-E]				
738.	[50901]	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.	[51100]	SI-11	<b>7.15.10 SI-11 – Error Handling [M]</b> [NIST 800-53, CMS MARS-E]				
740.	[51101]	SI-11a	The information system shall: a. Identify potentially security-relevant error conditions.	M			
741.	[51102]	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.	[51103]	SI-11c	c. Reveal error messages only to authorized personnel.	M			
743.	[51200]	SI-12	<b>7.15.11 SI-12 – Information Output Handling and Retention [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
744.	[51201]	SI-12a	a. The organization shall <b>handle and retain</b> 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.	[51900]	SI-99	This is a blank formatting line				
746.	[560000]	MP-00	<b>7.16 Media Protection (MP) Family</b>				
747.	[560200]	MP-01	<b>7.16.1 MP-1 – Media Protection P&amp;P [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
748.	ISO101	MP-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
749.	ISO102	MP-01a	a. A formal, documented media protection <b>policy</b> that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	L	In	a.	
750.	ISO103	MP-01b	b. Formal, documented <b>procedures</b> to facilitate the implementation of the media protection policy and associated media protection controls.	L	P	b.	
751.	ISO104	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.	ISO200	MP-02	<b>7.16.2 MP-2 – Media Access [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
753.	ISO201	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.	ISO202	MP-02b	b. Employ automated mechanisms to audit access attempts and access granted.	M		b.	
755.	ISO300	MP-03	<b>7.16.3 MP-3 – Media Marking [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E]				
756.	ISO301	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.	ISO302	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.	ISO400	MP-04	<b>7.16.4 MP-4 – Media Storage [M]</b>				
759.	ISO401	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.	ISO402	MP-04b	b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	M		b.	
761.	ISO500	MP-05	<b>7.16.5 MP-5 – Media Transport [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
762.		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.		MP-05b	b. Maintain accountability for information system media during transport outside of controlled areas.	M			
764.		MP-05c	c. Restrict the activities associated with transport of such media to authorized personnel.	M			
765.		MP-05d	d. Document activities associated with the transport of information system media.	M			
766.		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.		MP-06	<b>7.16.6 MP-6 – Media Sanitization [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA, IRS 1075]				
768.		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.		MP-06b	b. Employ sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	M		b.	
770.		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.		MP-06.1	Describe how the organization tracks, documents, and verifies media sanitization and disposal actions.	M			
772.		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.		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.		MP-06.6	Describe the organization's process for destroying media containing sensitive information that cannot be sanitized.	M			
775.		MP-07	<b>7.16.7 MP-ACA-1 – Media Related Records [M]</b> [CMS MARS-E]				
776.		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.	



[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
777.		MP-99	This is a blank formatting row.				
778.		IR-00	<b>7.17 Incident Response (IR) Family</b>				
779.		IR-01	<b>7.17.1 IR-1 – Incident Response P&amp;P [M]</b> [NIST 800-53, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]				
780.		IR-01	The organization shall develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:	L	P		
781.		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.		IR-01b	b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	L	P	b.	
783.		IR-02	<b>7.17.2 IR-2 – Incident Response Training [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
784.		IR-02a	The organization shall: a. Train personnel in their incident response roles and responsibilities with respect to the information system.	M		a.	
785.		IR-02b	b. Provide refresher training within every three-hundred-sixty-five (365) days.	M		b.	
786.		IR-03	<b>7.17.3 IR-3 – Incident Response Exercises [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				
787.		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.		IR-04	<b>7.17.4 IR-4 – Incident Handling [M]</b> [NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, HIPAA]				
789.		IR-04a	The organization shall: a. Implement an incident handling capability using Information Security Incident Handling and Breach Notification Procedures.	M			
790.		IR-04b	b. Coordinate incident handling activities with contingency planning activities.	M		a.	
791.		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.		IR-04d	d. Employ automated mechanisms to support the incident handling process.	M		c.	
793.		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.		IR-05	<b>7.17.5 IR-5 – Incident Monitoring [M]</b> [NIST 800-53, CMS MARS-E, IRS 1075]				

[sysname] Security Plan

IN	Priority	Cnt#	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
795.	170601	IR-05a	a. The organization tracks and documents information system security incidents.	M		a.	
796.	170602	IR-06	<b>7.17.6 IR-6 – Incident Reporting [M]</b> [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	<b>7.17.7 IR-7 – Incident Response Assistance [M]</b> [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	<b>7.17.8 IR-8 – Incident Response Plan [M]</b> [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.	

[sysname] Security Plan

IN	Priority	Cnt#	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.	170900	IR-99	This is a blank formatting row.				
811.	180000	AT-00	<b>7.18 Awareness and Training (AT) Family</b>				
812.	180100	AT-01	<b>7.18.1 AT-1 – Security Awareness Training P&amp;P [M]</b> [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 <b>policy</b> 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 <b>procedures</b> 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	<b>7.18.2 AT-2 – Security Awareness [M]</b> [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 <b>basic security awareness training</b> 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.	

[sysname] Security Plan

IN	Priority	Cntl #	Required Control	Risk	Stat	System Plan or Weakness Description	Resp. now
822.	180300	AT-03	<b>7.18.3 AT-3 – Security Training [M]</b> <i>[NIST 800-53, ISO 27001:2005, CMS MARS-E, 45 CFR Part 160, 162, 164, IRS 1075]</i>				
823.	180301	AT-03a	a. The organization shall provide role-based security-related training: <ul style="list-style-type: none"> <li>i. Before authorizing access to the system or performing assigned duties.</li> <li>ii. When required by system changes.</li> <li>iii. Refresher training within every three hundred sixty-five (365) days thereafter.</li> </ul>	M			
824.	180302	AT-03a2		M			
825.	180303	AT-03b	<i>[IRS 1075]</i> 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. <i>[SSA System Security Guidelines]</i> 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	<b>7.18.4 AT-4 – Security Training Records [M]</b> <i>[NIST 800-53, CMS MARS-E, IRS 1075]</i>				
828.	180401	AT-04a	The organization shall: <ul style="list-style-type: none"> <li>a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training.</li> </ul>	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	<input type="checkbox"/>			<input type="checkbox"/>	

## Appendix A – Vendor documentation

## Appendix B – Contracts, etc.

## Appendix C – Acronyms and Abbreviations

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

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

[sysname] Security Plan

Acronym	Term
DPA	Division of Public Assistance
DR	Disaster Recovery
DSO	Department Security Office
EIS-R	Eligibility Information System – Replacement
EPHI	Electronic protected health information
ESI	Electronically Stored Information
FIPS	Federal Information Processing Standards
FTI	Federal Tax Information
GSS	General Support Systems
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
HTTPS	Hypertext Transfer Protocol Secure
IA	Identification and Authentication
ID	Identifier
IDS	Intrusion detection system
INR	Incident Response Report
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
IRS	Internal Revenue Service
IRT	Incident Response Team
IS	Information Security
ISO	International Organization for Standardization
IT	Information Technology

Acronym	Term
SA	System and Services Acquisition
SAR	Safeguard Activity Report
SAM	Security Access Manager
SC	System and Communications Protection
SDLC	Software Development Lifecycle
SFTP	Secure File Transfer Protocol
SI	System and Information Integrity
SOA	State Of Alaska
SSA	Social Security Administration
SSL	Secure Sockets Layer
SSN	Social Security Number
SSO	State Security Office
SSP	System Security Plan
TLS	Transport Layer Security
URL	Uniform Resource Locator
USGCB	U.S. Government Configuration Baselines
VLAN	Virtual Local Area Network
VM	Vulnerability Management
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Points
WP	Worker Portal