

Centers for Medicare & Medicaid Services Information Security and Privacy Group

Risk Management Handbook (RMH) Chapter 12: Security & Privacy Planning

Final

Version 1.0

January 31, 2017

Record of Changes

The "Record of Changes" table below should be used to capture changes when updating the document. All columns are mandatory.

Version Number	Date	Author/Owner Name	Description of Change
1.0	01/31/2017	CMS ISPG	Initial Release

Effective Date/Approval

This policy becomes effective on the date that CMS's Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified, or superseded by another policy.

Signature:	/s/	Date of Issuance:	1/31/2017	
	George Hoffman			
	Acting Chief Information Officer			
	and Director, Office of Enterprise			
	Information (OEI)			

Policy Owner's Review Certification

This document shall be reviewed in accordance with the established review schedule located on the CMS website.

		Date of Annual	
Signature:		Review:	
	Emery Csulak	-	
	CMS Chief Information Security Officer		
	and Senior Official for Privacy		

Table of Contents

1.	Pur	pose	6
	1.1	Authority	6
	1.2	Scope	
	1.3	Handbook Structure	7
	1.4	Background	7
	1.5	Policy	8
	1.6	Standards	10
	1.7	Guidelines	10
2.	Rol	es and Responsibilities	10
		cedures	
	3.1	System Security Plan (PL-2)	
	0.1	3.1.1 System Name and Identifier	
		3.1.2 Security Categorization	
		3.1.3 System Points of Contact (POCs)	
		3.1.4 Authorization Boundary	
		3.1.5 System Interconnection/Information Sharing	17
		3.1.6 Security Control Selection	18
		3.1.7 Documenting Security Control Implementations	20
		3.1.8 System Security Plan Approval	
		3.1.9 System Security Plan Update and Maintenance	
		3.1.10 System Security Plan Dissemination	
	3.2	Plan/Coordinate with Other Organizational Entities (PL-2(3))	
	3.3	Rules of Behavior (PL-4)	
	3.4	Social Media and Networking Restrictions (PL-4(1))	
	3.5	Information Security Architecture (PL-8)	27
Aı	pen	dix A. Acronyms	28
Aı	pen	dix B. Glossary of Terms	30
Aı	pen	dix C. Applicable Laws and Guidance	36
Aı	pen	dix D. Feedback and Questions	41
Aı	pen	dix E. ARS Standards – Planning (PL)	42
Δ 1	men	div F. Control/Policy Cross Reference Table	40

Tables

Table 1: CMS Defined Parameters – Control PL-2	12
Table 2: CMS Defined Parameters – Control PL-2(3)	25
Table 3: CMS Defined Parameters – Control PL-4	26
Table 4: CMS Defined Parameters – Control PL-8	27

1. Purpose

The Centers for Medicare and Medicaid Services (CMS) RMH Chapter 12: Security & Privacy Planning is written in compliance with the CMS Information Systems Security and Privacy Policy (IS2P2) and the CMS Information Security Acceptable Risk Safeguards (ARS). The intent of this chapter is to document standard operating procedures that facilitate the implementation of security and privacy controls associated with the Planning (PL) control family taken from the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations and tailored to the CMS environment in the CMS ARS.

1.1 Authority

The Office of Management and Budget (OMB) designated the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) as authorities to provide guidance to federal agencies for implementing information security and privacy laws and regulations, including the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, the *Privacy Act of 1974* ("*Privacy Act*"), and the *Federal Information Security Modernization Act (FISMA) of 2014*. In addition, the *CMS Information Systems Security and Privacy Policy (IS2P2)* defines the framework under which CMS protects and controls access to CMS information and information systems in compliance with federal law.

Per the Department of Health and Human Services (HHS) Information Systems Security and Privacy Policy (IS2P), the CMS Chief Information Officer (CIO) designates the CMS Chief Information Security Officer (CISO) as the CMS authority for implementing the CMS-wide Information Security and Privacy program. This policy also designates the Senior Official for Privacy (SOP) as the CMS authority for implementing the CMS-wide privacy program. Through the policy, the CISO/SOP delegate authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy program. All CMS stakeholders must comply with and implement controls as outlined in this handbook to ensure compliance with federal requirements and programmatic policies, standards, procedures, and to facilitate the implementation of information security and privacy controls.

1.2 Scope

This handbook documents procedures which facilitate the implementation of the security controls and standards defined in the CMS IS2P2¹ and the CMS ARS² for the PL control family. This handbook is intended for use by CMS employees and contractors who support the development, operations, maintenance, and disposal of CMS information systems. This document was written to address the high baseline of security controls in accordance with NIST-SP 800-53 Revision 4 (NIST 800-53r4). Therefore there may be security controls include within

¹ For more information on CMS IS2P2 go to https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS2P2.pdf

² For more information on CMS ARS go to https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

this document that might not apply to information systems with a lessor categorization (i.e. moderate or low). This handbook does not supersede any other applicable law, higher-level agency directive, or existing labor management agreement.

1.3 Handbook Structure

This handbook is designed to align with the NIST-SP 800-53 Revision 4 (NIST 800-53r4) *Security and Privacy Controls for Federal Information Systems and Organizations* catalogue of controls,³ the CMS IS2P2, and the CMS ARS. Each procedure is related to a specific NIST security control and additional sections have been included in this document to increase traceability and to satisfy audit requirements.

This document is organized by sections and appendices as follows:

- Purpose
 - Authority
 - Scope
 - Handbook Structure
 - Background
 - Policy
 - Standards
 - Guidelines
- Roles and Responsibilities
- Procedures
- Related Controls
- Appendices
 - Appendix A: Acronyms
 - Appendix B: Glossary of Terms
 - Appendix C: Applicable Laws and Guidance
 - Appendix D: Feedback and Questions
 - Appendix E: ARS Standards Planning (PL)
 - Appendix F: Control/Policy Cross Reference Table

1.4 Background

NIST-SP 800-53r4 states under the PL control family that an organization develops, disseminates, and must periodically review and update its planning documentation. This

³ For more information on NIST-SP 800-53r4 go to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

includes a formal, documented, security and privacy planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the security and privacy planning policy and associated security and privacy planning controls.

This *RMH Chapter 12: Security and Privacy Planning* provides procedures that assist with the implementation of the PL family of controls to ensure information security and privacy planning for FISMA systems within the CMS enterprise environment and on any systems storing, processing, or transmitting CMS information on behalf of CMS. This control family addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

1.5 Policy

An information security and privacy policy is a set of high-level statements that protect information across an organization. The CMS IS2P2 defines the framework and policy under which CMS protects and controls access to CMS information and information systems in compliance with HHS policy and federal law. Specifically, the CMS IS2P2 outlines the following policies for the PL family of controls:

- PL-1 The Program must develop and maintain the PL family of controls to ensure information security and privacy planning for FISMA systems are performed within the CMS enterprise environment and on any systems storing, processing, or transmitting CMS information on behalf of CMS. The Program must:
 - PL-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the PL family of controls in the ARS to:
 - PL-1.1.1 Develop, document, and maintain information security and privacy plans for each CMS system and network:
 - PL-1.1.1.1 Security plans must be in accordance with NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems.⁴
 - PL-1.1.1.2 Privacy plans must address the privacy requirements for confidentiality, availability, and integrity for the organization and individual information system(s)
 - PL-1.1.1.3 Business Owners/ISOs must review and update the information security and privacy plans periodically as defined in the ARS or when significant changes occur to the system/network
 - PL-1.1.2 Develop, document, and maintain an Information Security Architecture to:

_

⁴ For more information on NIST SP 800-18 go to http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

- PL-1.1.2.1 Document the information security segments of the CMS enterprise architecture in accordance with OMB Circular A-130⁵
- PL-1.1.2.2 Fully integrate information security and privacy into the CMS architecture framework
- PL-1.1.2.3 Provide an architecture framework consistent with HHS's Enterprise Architecture program and based on the taxonomy of the Federal Enterprise Architecture Framework
- PL-1.1.3 Review and update the security segments of the CMS enterprise architecture periodically, as defined in the ARS
- PL-1.1.4 Develop, document, and maintain the CMS Acceptable Use standards within the CMS Policy for the Acceptable Use of CMS Desktop/Laptop and Other Information Technology (IT) Resources
 - PL-1.1.4.1 Privacy requirements must be identified in contracts and acquisition-related documents.
 - PL-1.1.4.2 CMS employees and contractors (users) must:
 - PL-1.1.4.2.1 Be informed that the use of CMS IT resources, other than for authorized purposes, is a violation of the HHS Rules of Behavior (For Use of HHS Information Technology Resources) and the HHS Policy for Personal Use of Information Technology Resources and is grounds for disciplinary action, up to and including removal from federal service, monetary fines, and/or criminal charges, which could result in imprisonment
 - PL-1.1.4.2.2 Be prohibited from transmitting sensitive CMS information using any non-CMS approved Internetbased mechanism, including but not limited to personal email, file-sharing, file transfer, and backup services
 - PL-1.1.4.2.3 Read and sign the HHS Rules of Behavior (RoB) periodically, as defined in the ARS
 - PL-1.1.4.3 Personal use of CMS IT resources must comply with HHS Policy for Personal Use of Information
 Technology Resources, which governs the appropriate use of CMS IT resources to ensure personal use of those resources does not put CMS data at risk of unauthorized disclosure or dissemination
- PL-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Planning family of controls

Version 1.0

⁵ For more Information on OMB Circular A-130 go to http://www.whitehouse.gov/omb/circulars a130 a130trans4/

1.6 Standards

Standards consist of specific security control implementation requirements that enforce and support the Information Security and Privacy policy. The CMS ARS defines CMS specific standards for each of the required NIST 800-53r4 security controls in compliance with HHS policy and the CMS IS2P2. A copy of the CMS ARS standards for the PL family of controls is outlined in Appendix E.

1.7 Guidelines

Guidelines are recommended non-mandatory controls that help support the standards or serve as a reference when no standard exists. Guidelines provide guidance and best practices relative to a particular topic. Guidelines may accompany, interpret, or provide guidance for implementing CIO policies, or may provide guidance to various CMS IT Life Cycle activities. Guidelines are recommended best practices but are not required to comply with policy. A guideline aims to streamline particular processes according to a set routine or sound practice. All applicable guidelines for the PL family can be found in Appendix C of this document.

2. Roles and Responsibilities

A comprehensive list of information security and privacy roles and responsibilities for CMS stakeholders is contained in Section 3 Roles and Responsibilities of the CMS IS2P2. The following roles from the CMS IS2P2 are specific to the procedures contained within this handbook. These roles represent a baseline for a comprehensive security and privacy team.

- Chief Information Security Officer (CISO)
- Information System Security Officer (ISSO)
- Cyber Risk Advisor (CRA)
- Data Guardian (DG)
- Information System Owner (ISO)
- Business Owner (BO)
- Chief Information Officer (CIO) / Authorizing Official (AO)
- Senior Official for Privacy (SOP)

3. Procedures

Procedures provide detailed instructions on how to implement specific security controls and meet the criteria defined in standards. This section contains the applicable procedures that facilitate the implementation of the PL family security controls as required by the CMS IS2P2 and the CMS ARS. To increase traceability, each procedure has been mapped to the associated NIST controls using the control number from the CMS IS2P2. Appendix F Control/Policy Cross Reference Table shows the relationship between the NIST 800-53r4 PL Controls, CMS ARS PL Controls, CMS IS2P2 Policy, and HHS IS2P Policy.

3.1 System Security Plan (PL-2)

The purpose of a System Security Plan (SSP) is to provide an overview of the security requirements of a system and describe the controls that are in place or planned to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. Creation of the SSP represents a structured process of planning adequate and cost-effective security protection for a system.

At CMS, a SSP is a single document generated by the CMS Federal Information Security Management Act Controls Tracking System (CFACTS). A CFACTS generated SSP relates the CMS security requirements defined in the CMS IS2P2 to a set of security controls and control enhancements as outlined in the CMS ARS. The CFACTS SSP also describes, at a high level, how the security controls and control enhancements meet those security requirements.

In order to ensure the SSP reflects adequate protection of the information resources, a senior management official must authorize a system to operate. The authorization of a system is granted by an Authorizing Official (AO) and is an important quality control. By authorizing the processing of a system, the AO accepts its associated risk. Authorization should be based on an assessment of management, operational, and technical controls. Since the SSP establishes and documents the security controls, it should form the basis for the authorization, supplemented by the Security Assessment Report (SAR) and the Plan of Actions and Milestones (POA&M).

All CMS information systems must develop and maintain a SSP, which must be compliant with current CMS guidelines, consistent with the CMS Technical Reference Architecture (TRA), and tracked by the CMS CFACTS tool. SSP development should begin for an information system during the Initiation, Concept, and Planning phase of the CMS Expedited Lifecycle (XLC) as this will ensure that security controls are integrated during the development of the system. The following sub-sections contain the detailed procedures describing how to complete the various sections of the SSP using the CMS CFACTS tool.

The table below outlines the CMS organizationally defined parameters (ODPs) for this control.

Table 1: CMS Defined Parameters – Control PL-2

Control	Control Requirement	CMS Parameter
PL-2	b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];	 b. Applicable plan stakeholders to include: System Developers/Administrators Business Owner Chief Information Officer/Authorizing Official Cyber Risk Advisor Information System Owner Information System Security Officer Senior Official for Privacy Contingency Personnel Incident Response Personnel
	 Reviews the security plan for the information system [Assignment: organization-defined frequency]; 	c. At least every 365 days

3.1.1 System Name and Identifier

Each new system must be identified in CFACTS through the assignment of a system Unique Identification Number (UID). The UID associates the system to an authorization package. The system UIDs are critical to the successful reporting of information HHS-wide, therefore, the process of assigning a new UID to an Authorization Package is limited to specific Information Security and Privacy Group (ISPG) staff.⁶ The following steps detail the CMS specific process for the creation of the system UID and the assignment of that ID to an Authorization Package in CMS CFACTS:⁷

• **Step 1:** Overall assignment of the UID number is owned by the Division of Enterprise Architecture (DEA).⁸ The DEA, within the Strategy and Architecture Group (SAG)⁹ and the Office of Enterprise Information (OEI),¹⁰ creates the UID in the HHS Enterprise

⁶ Security and Privacy Group (ISPG) staff can be contacted through the CISO mail box at CISO@cms.hhs.gov

Very must be authorized to use CFACTS and must utilize the VPN if accessing from outside of the CMS network. https://cfacts.cms.local/

⁸ For more information on CMS DEA go to https://www.cms.gov/About-CMS/Agency-Information/CMSLeadership/Office-OEI.html

⁹ For more information on the CMS SAG go to https://www.cms.gov/About-CMS/Agency-Information/CMSLeadership/Office-OEI.html

¹⁰ For more information on the CMS OEI go to https://www.cms.gov/About-CMS/Agency-Information/CMSLeadership/Office-OEI.html

- Architecture Repository (HEAR),¹¹ where the overall/master CMS inventory is maintained
- **Step 2:** DEA then forwards the UID to the various other inventory maintainers within CMS. One of these stakeholders is ISPG which maintains a system inventory in CFACTS
- **Step 3:** The Cyber Risk Advisor (CRA) adds or updates the UID within the CFACTS tool for the information system
- Step 4: The CRA notifies the ISSO and the Business Owner via email that the UID has been assigned to the information system and that an authorization package may now be developed using CFACTS

3.1.2 Security Categorization

Each new system must define its security categorization within CFACTS. Before the system security plan can be developed, the information system and the information resident within that system must be categorized based on the *Federal Information Processing Standards Publication 199* (FIPS 199). NIST Special Publication 800-60 Revision 1 Volume I: *Guide for Mapping Types of Information and Information Systems to Security Categories* a guideline for mapping types of information and information systems to security categories and was written to work in conjunction with FIPS 199. CMS currently utilizes eleven of the data types listed in NIST Special Publication 800-60 and has configured the CFACTS tool to only display these data types. Authorization boundaries are also developed and reviewed in correlation with the security categorization as the boundary has a direct effect on the categorization of the system. The security categorization for an information system is completed by the ISSO and approved by the Information System Owner. The following steps detail the CMS specific process for conducting a security categorization on an information system using CFACTS:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu
- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system

For more information on HEAR logon to the CMS network and go to <a href="http://search.hhs.gov/search?q=HHS+Enterprise+Architecture+Repository+%28&HHS=Search&site=HHS&entqr=3&ud=1&sort=date%3AD%3AL%3Ad1&output=xml_no_dtd&ie=UTF-8&oe=UTF-8&Ir=lang_en&client=HHS&proxystylesheet=HHS

¹² For more information on system categorization and FIPS 199 go to http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

¹³ For more information on information type and NIST 800-60 Volume I go to http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

- **Step 5:** Select the "Security Category" tab from the top navigation tab of the authorization package
- Step 6: Click "Edit" at the top of the authorization package window
- **Step 7:** Answer the following question in the Organizational Users Section "Is this system accessed by non-organizational users?"
 - For help determining who is considered an organizational user and a nonorganizational user see the help text by clicking on the question mark to the left of the question
- Step 8: Select the information types processed, stored or transmitted by the system
 - In the Information Type section click on the right hand side of the "*Lookup*" title bar in the upper right hand corner
 - o In the "*Record Lookup*" pop up select the checkbox to the left of each information type that is used by your information system
 - Click "Ok" when done
- **Step 9**: Click the "Save" at the top of the screen to save all changes

3.1.3 System Points of Contact (POCs)

CMS must maintain system points of contact (POC) for all systems. This contact information is maintained in the CFACTS database and is updated via the stakeholders section which is located on the General tab for an information system. It is the responsibility of the ISSO to input and maintain the POCs using the CFACTS tool. The following steps detail the CMS specific process for maintaining POCs in CFACTS:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu
- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system
- Step 5: Select the "General" tab from the top menu of the authorization package
- **Step 6:** To edit the stakeholder information you must first click the "*Edit*" button (top left of authorization package) and then scroll down to the stakeholders section¹⁴ (third one down)
- **Step 7:** Update the stakeholder information and click "Apply"

¹⁴ Section 4.2.3 of the CFACTS User's Manual contains a screenshot of the stakeholders screen as well as additional information on selecting each role.

Note: Points of contact should be identified for the following roles:

- o Business Owner
- o Primary ISSO
- System Developer and Maintainer (SDM)
- ISSO Contractor Support (ISSOCS)
- o CIO
- o CISO
- Deputy CISO
- Security Control Assessor (SCA)
- o CRA

3.1.4 Authorization Boundary

Definition of the authorization boundary is a critical first step in the authorization process and directly affects the security categorization of a system. The FIPS 199 impact levels must be considered after the system's description, purpose, and boundaries are documented and will determine the initial baseline set of security controls that will be applicable to the information system. The authorization boundary is defined as all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.¹⁵

CMS must explicitly define the authorization boundary for the system. The characteristics of an authorization boundary are:

- A set of information resources allocated to an information system
- Information resources that consist of information and related resources including personnel, equipment, funds, and information technology
- If a set of information resources is identified as an information system, the resources are generally under the same direct management control

A detailed description of the authorization boundary and the system's technical components must be supplied and loaded into CFACTS. CFACTS does not automatically define the authorization boundaries of a system. In CFACTS, the authorization boundary is defined by a combination of network/boundary drawings, hardware and software inventories, interconnections, and a narrative. The authorization boundary should be defined before completing the security categorization in CFACTS as it has a direct effect on the categorization of the system.

System Description/Purpose:

A key component of a well-defined authorization boundary is a narrative describing the general description and purpose of the system. The following steps detail the process for loading the general description/purpose into CFACTS:

• **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu

¹⁵ Taken from NIST SP 800-37 revision 1 go to http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

- Step 2: Expand "Authorization Package" from the left hand navigation menu
- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located, click on the system name to open the authorization package for the system
- Step 5: Select the "General" tab from the top menu of the authorization package.
- **Step 6:** Click "Edit" at the top of the CFACTS page, the General Tab has a section marked "Information System Details"
- **Step 7:** Populate the "System Description" field with a description of the purpose of the system. Be sure to describe which CMS business process the system supports or which function the system performs. Also list all applications associated with the information system and describe each application's function. Include a list of user organizations and specify whether the users are internal or external to the system owner's component/organization
- **Step 8:** Click "Apply" in the upper left hand corner of the Authorization Package screen to save the change

System Environment:

The system environment describes the technical system to include the primary hardware, software, and communications equipment. It should also include any environmental or technical factors that raise special security concerns, such as use of mobile devices, wireless technology, etc. The following steps detail the process for adding the system environmental description in CFACTS:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu
- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system
- Step 5: Select the "Boundary" tab from the top menu of the authorization package
- **Step 6:** Click "Edit" at the top of the CFACTS page
- Step 7: Add the system environmental description in the "Boundary Description" field
- **Step 8:** Click "Apply" in the upper left hand corner of the Authorization Package screen to save the changes

- **Step 9:** Under the "Boundary Diagrams" section, attach network, dataflow, and boundary diagrams by clicking the "Add New" link. In order to have this information appear in the SSP, the uploaded documents must be Microsoft Word (.doc or .docx) documents. Any images or diagrams must be incorporated into the uploaded Word document(s) to be displayed in the SSP. You may use more than one Word document in this section but it is recommended to incorporate everything into a single Word document"
- **Step 10:** Populate the "*Hardware*" section by clicking the "*Add New*" link and completing all fields. The hostname field is particularly important as it will be used to support continuous monitoring activities such as automated vulnerability scanning. Be sure to create an entry for all hardware assets associated with the authorization boundary
- **Step 11:** Click "Apply" in the upper left hand corner of the "Authorization Boundary" screen to save the changes

3.1.5 System Interconnection/Information Sharing

A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. ¹⁶ A system interconnection is documented in an Interconnection Security Agreement (ISA) and a Memorandum of Understanding/Agreement (MOU/A). The ISA and Memorandum of Understanding (MOU) are similar documents with the same basic purpose. While the ISA tends to be a technical document, the MOU is a business agreement, but these differences are not necessarily meaningful enough to warrant that both documents are prepared in all cases. Typically, only very complex interconnections that are a component of a broader business relationship would require a MOU in addition to an ISA. A MOU should not be necessary for most HHS systems, provided the ISA sufficiently documents the technical requirements for, and defines the roles/responsibilities in managing, the interconnection. CFACTS provides a mechanism for inventorying interconnections for CMS information systems and also provides a location to store and maintain the associated ISA and MOU/A for each. The following steps describe a detailed process for entering interconnections and uploading the associated agreements into CFACTS:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu
- Step 3: Click on "Records" and select the appropriate information system. You may also find the information system by clicking "Search Records" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system

Risk Management Handbook (RMH) Chapter 12: Security & Privacy Planning Version 1.0

¹⁶ For more information on system interconnections go to http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

- Step 5: Select the "Boundary" tab from the top menu of the authorization package
- **Step 6:** To edit the interconnection information you must first click the "*Edit*" button (top left of authorization package) and then scroll down to the "*Interconnections*" section ¹⁷(bottom section)
- **Step 7:** Click the "Add New" link
- **Step 8:** Populate all of the fields of the "Interconnection Information" section
- **Step 9:** Upload any associated ISA or MOU by clicking the "Add New" link in the top right of the "Interconnection Authorization Documentation" section, browse to and select the file, and click "open," to look up and fill in the information systems section. If the users fill in the interconnection type field with external, a new section called interconnection third party is added. This section also needs to be completed when it is applicable
- **Step 10:** Click "Apply" in the upper left hand corner of the "Interconnections: Add New Record" screen to save the changes

3.1.6 Security Control Selection

For each information system, the appropriate baseline of security controls is automatically allocated by CFACTS based on the information system's defined security category. For this reason, the security category must be completed for the information system prior to tailoring the security controls. Refer to section 3.1.2 above for the procedures to complete the security categorization.

For control allocation and tailoring CFACTS implements the following characterizations of security controls:

- Common Controls: Common Controls are security controls whose implementation results in a security capability that is inheritable by one or more organizational information systems. Security controls are deemed inheritable by information systems or information system components when the systems or components receive protection from the implemented controls but the controls are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the systems or components—entities internal or external to the organizations where the systems or components reside
- Hybrid Controls: Hybrid Controls are security or privacy controls that is implemented in an information system in part as a common control and in part as a system-specific control
- System Specific Controls: System Specific Controls are security controls for an information system that have not been designated as a common security control or the portion of a hybrid control that has to be implemented within an information

¹⁷ Section 4.4.5 of the CFACTS User's Manual contains a screenshot of the interconnections screen as well as additional information on interconnections.

¹⁸ Section 4.5.4 of the CFACTS User's Manual contains more information on security control allocation.

system. System-specific controls are the primary responsibility of information system owners

• **Allocated Controls:** CFACTS identifies Allocated Controls are those controls attributed/assigned to the information system

It is possible in CFACTS to tailor the initial baseline of security controls. Tailoring activities consist of adding additional controls for extra security based on an assessment of risk, identifying controls that are not applicable using scoping guidance, and by applying common and hybrid controls. Once tailoring activities have been completed, the tailored set of security controls provides an overview of the security requirements for the system. The following steps detail the CMS specific process for allocating and tailoring the initial baseline of security control in CFACTS:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu
- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system
- Step 5: Select the "Controls" tab from the top menu of the authorization package
- Step 6: Under the "Allocate Baseline Controls" section, in edit mode, click the radio button labeled "Ready to Allocate". When this radio button is selected a button labeled "Allocate Controls" will appear on the right side of the section. Click this button to allocate the initial baseline of security controls. It is important to note that prior to allocating baseline security controls to an information system the "Security Category" tab and the "Boundary" tab must be completed. See sections 3.1.2 and 3.1.4 above for instructions for completing these sections. After the clicking the "Allocate Controls" button the process will take several minutes to complete and the screen will need to be refreshed before the security controls will show up in a list under the "Allocated Controls" section. It is a good idea to Save and close the record at this point. The user can open the record and the Controls tab again once they have waited long enough for the internal process to create the controls list for this Authorization Package
- **Step 7:** To tailor a security control identify the control from the list of allocated controls and click on the control number
- **Step 8:** Under the "Allocated Controls" box click the "Edit" button in the upper left hand corner
- **Step 9:** Scroll down to the "Control Allocation" section and select "Inherited" to apply a common control or "Not Applicable" if the control does not apply to the information system. If a status of "Not Applicable" is selected then a "Reason For De-allocation" dialogue box will appear to the right. This field must be completed and should contain an

explanation of why the control is not required for the information system. If a status of "Inherited" is selected then the user must complete the "Control to Inherit" section by clicking the "Lookup" link in the upper right hand corner of that section and selecting the security control and authorization package providing the control from the list

- **Step 10:** Click "Save" to apply the tailoring for that control and return to the list of allocated controls
- **Step 11:** To add a control that was not allocated as a result of the initial allocation described above in Step 6, if the user wishes to add a control that CFACTS did not allocate, the user will have to make a request to have that control added to the system Authorization Package
- **Step 12:** Under the "Allocated Controls" box click the "Edit" button in the upper left hand corner
- Step 13: Scroll down to the "Control Allocation" section and select "Allocated"
- **Step 14:** Click "Save" to apply the tailoring for that control and return to the list of allocated controls

3.1.7 Documenting Security Control Implementations

All Business Owners and ISSOs are required to maintain a current SSP for the information systems within CFACTS. For each applicable security control, the SSP should indicate whether the control is satisfied or other than satisfied, describe how the control is implemented, and include a rationale for any tailoring decisions that have been applied to the control. A comprehensive security control implementation description should:

- Address all the requirements of the control
- Describe how each requirement and objective is met with enough detail to permit the testing of the control
- Describe the desired outcome/expected behavior of the control
- Describe where any associated process or procedures that support the controls implementation are maintained
- Identify the responsible party for ensuring that the control is properly implemented and operating as intended

It should be noted that because of the complexity of the CMS architecture many systems include multiple diverse sub-systems and/or components that may be managed and accessed by different groups depending on how the service is architected. Because of this it is important that each sub-system and/or components address the control implementation description identified in the bullet points above.

The following steps detail the CMS specific steps for documenting security control implementation descriptions using CFACTS:

• Step 1: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu

- Step 2: Expand "Authorization Package" from the left hand navigation menu
- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system
- **Step 5:** Navigate to the "Controls" tab
- Step 6: Ensure that the controls have been allocated as described in section 3.1.6
- Step 7: Select a control by clicking on that control
- **Step 8:** Determine the Allocation Status of the control if not already done in section 3.1.6. Click "*Edit*" on the top of the screen
- **Step 9:** In the Control Allocation section, select the "*Allocated*", "*Inherited*" or "*N/A*" radio button. Allocated controls require that all control implementation is provided by the system. Inherited controls can either be fully inherited or hybrid. Fully inherited controls inherit all the control implementation from another control provider. Hybrid controls only inherit a portion of the control and are responsible for what is not inherited
- **Step 10:** Determine if your system is a common control provider to other systems and is providing this control for inheritance
- **Step 11:** In the Implementation section click on the radio button of the appropriate selection for Inheritable, "Yes", "No"
- **Step 12:** Determine if your system is providing a portion of the control or all of the control for inheritance. If providing only a portion of the control, click the radio button for a hybrid control, "Yes", otherwise click "No"
- **Step 13:** In the "Private Allocated Controls Information" section click "Add New"
- **Step 14:** Clicking on the "Add New" in Step 13 opens the "Private Allocated Control Information: Add New Record" screen, in the screen, the user will document descriptions using the criteria listed in the three bullet points above. Click "Save" at the top
- Step 15: If you are providing this as an inheritable control, in the Shared Implementation Details area, document the portion of the control that is being provided to other systems. It is advisable to specifically callout whether the control is a Hybrid or not and specially state in the Shared Implementation Details what the provider is doing and what the inheriting system is required to do to fully satisfy the control
- **Step 16:** Click "Save" at the top

3.1.8 System Security Plan Approval

NIST SP 800-53 v4 requires that the SSP be approved by the AO or his/her designee. CMS does this through the CFACTS tool which requires the ISSO, SDM and Business Owner to approve

the plan. The approval for a SSP occurs after the SSP has been reviewed and updated as part of the ATO process.

The SSP is finalized as part of the ATO process. This occurs after all the information contained within the "General", "Security Category", "Boundary" and "Controls" tabs in CFACTS has been documented, reviewed and/or updated and the SSP has been generated. Approval of the SSP occurs after a formal security control assessment has been conducted, approved by the CMS ATO review team, and the CMS System Certification Authorization to Operate (ATO) certificate form has been signed by the ISSO, SDM and Business Owner.

ATO Package/SSP Submittal for Approval:

The following steps detail how to retrieve the documentation and submit the ATO Package which includes the SSP for review and approval:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu
- Step 3: Click on "Records" and select the appropriate information system. You may also find the information system by clicking "Search Records" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system
- Step 5: Download the following documents from the appropriate tab
 - System Security Plan Authorization tab
 - Security Assessment Plan Authorization tab
 - Security Assessment Report Authorization tab
 - Privacy Impact Assessment (PIA) Security Tab
 - Interconnection Security Agreement (ISA) Boundary tab
 - Information System Risk Assessment (ISRA) Security Category tab
 - Contingency Plan (CP) Security Category tab
 - CP Test Plan Security Category tab
 - CP After Action Report Security Category tab
 - Ensure that all POA&Ms for the system are up to date within CFACTS
- **Step 6:** Review all security documents to ensure the documents are complete, up to date and have been reviewed, approved, and signed
- **Step 7:** Complete the CMS System Certification Authorization to Operate (ATO) Request Form and have the ISSO, SDM and Business Owner sign it
- Step 8: On the Authorization tab click "Edit" at the top

- **Step 9:** Upload the CMS System Certification Authorization to Operate (ATO) Request Form to the Certification Form section of the Authorization tab in CFACTS
- **Step 10:** In the Authorization Decision section select "Submitted" from the pull down menu in the Authorization Package Submission Status
- **Step 11:** Click "Save" at the top

Documenting the SSP Approval:

Once the Authorization Package has been submitted, the AO reviews the package and renders a decision. Since the SSP is a key component of the ATO package, receipt of an ATO also serves as a formal approval of the SSP. This decision is documented in CFACTS and an Authorization Memo is signed by the AO and must be uploaded into CFACTS by the CRA. The following steps detail how to upload the Authorization Memo into CFACTS which serves as an artifact demonstrating the SSP approval. This process assumes that the CRA has already scanned the document and has an electronic version available:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu
- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system
- **Step 5:** Click on the "Authorization" tab
- **Step 6:** Click "Edit" at the top of the CFACTS page
- **Step 7:** Click "Add" to the right of the "Authorization Memo" in the Authorization Decision section of the Authorization tab
- **Step 8:** Click "*Browse*" and select the authorization memo for the system. Click "*Select Files*" after clicking add
- **Step 9:** Click "*OK*"
- **Step 10:** Click "Save" at the top

3.1.9 System Security Plan Update and Maintenance

The CMS IS2P2 and the ARS require Business Owners to review and update the SSP at least annually. The following steps detail the process for updating the SSP using the CFACTS tool:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
- Step 2: Expand "Authorization Package" from the left hand navigation menu

- **Step 3**: Click on "*Records*" and select the appropriate information system. You may also find the information system by clicking "*Search Records*" and specifying search criteria
- **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system
- Step 5: Perform a comprehensive review of all the data and fields in the following tabs:
 - General
 - Security Category
 - Boundary
 - Controls
- **Step 6**: Go to the Authorization tab and ensure that "*Pre-assessment Progress Review*" section has green check marked for the following items:
 - Authorization Boundary
 - Security Category
 - Allocated Controls
 - Defined Implementation Details
- Step 7: Click on the button "Generate SSP" in the System Security Plan (SSP) section
- **Step 8**: When the Authorization Package: Export Options window opens generate your SSP using the System Security Plan (SSP) Report Template in Microsoft® Word
- Step 9: Review the generated SSP for completeness and accuracy
- Step 10: Upload the SSP to the System Security Plan (SSP) Attachments area of the System Security Plan (SSP) section. Use the following naming convention {System Name}_SSP_(date generated) e.g. OCISO Inheritable Controls_SSP_04252016

3.1.10 System Security Plan Dissemination

The SSP should be disseminated to all applicable stakeholders for the information system to include the following:

- System Developers/Administrators
- Business Owner
- Chief Information Officer/Authorizing Official
- Cyber Risk Advisor
- Information System Owner
- Information System Security Officer
- Senior Official for Privacy
- Contingency Personnel
- Incident Response Personnel

Dissemination should be handled in a timely manner such as when the SSP has been reviewed and/or updated. The latest SSP can be downloaded and reviewed via CFACTS. Security plans should be distributed only on a need-to-know basis. Since the SSP is a sensitive security document that requires special handling, it should only be distributed to those stakeholders who have a need to know. The preferred method to disseminate the SSP is through granting CFACTS access to those stakeholders so these stakeholders can view all relevant information online.

3.2 Plan/Coordinate with Other Organizational Entities (PL-2(3))

CMS must plan and coordinate security-related activities impacting the information system with the affected internal or external stakeholders, groups, or organizations before conducting such activities in order to reduce the impact on other CMS organizational entities. These stakeholders, groups, or organizations could include those involved with security-related activities, or providing services or support (such as Trusted Internet Connection (TIC), or those involved in COOP planning). The table below outlines the CMS organizationally defined parameters (ODPs) for this control.

Table 2: CMS Defined Parameters – Control PL-2(3)

Control	Control Requirement	CMS Parameter
PL-2(3)	(3) The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.	 (3) Stakeholders associated with the following security related activities: Security Control Assessments (SCAs) Audits (e.g. Chief Financial Officer (CFO) Audits, and Annual FISMA) Automated Vulnerability Scanning Activities Associated with Continuous Diagnostics and Mitigation (CDM) Training Hardware and Software Maintenance Patch Management/Configuration Management Contingency Plan/Information Technology Continuity Plan (CP/ITCP) Testing Incident Response Testing

The following steps detail a process for coordinating security related activities with internal and external stakeholders.

- Step 1: Identify all the relevant stakeholders for the security related activity
- **Step 2**: Establish a primary method of communication. Possible methods of communication include emails, face to face meetings, and teleconferences

- Step 3: Communicate with all relevant stakeholders using the primary method of communication identified in Step 2 above. Introduce the security related activity and describe the areas for which you are requesting input/support from each stakeholder. Be sure to generate an artifact documenting this interaction (e.g. email trails, meeting minutes, etc.)
- **Step 4**: Issue follow up communications as necessary. You may use other methods of communication aside from the primary method identified in Step 2 but you must generate an artifact documenting the interaction (e.g. email trails, meeting minutes, etc.)

3.3 Rules of Behavior (PL-4)

Rules of Behavior (RoB) clearly delineates responsibilities and the expected behavior of all individuals with access to the system. The table below outlines the CMS organizationally defined parameters (ODPs) for this control.

Control	Control Requirement	CMS Parameter
PL-4	c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency];	c. Reviews and updates the Rules of Behavior at least every three years. Users must acknowledge the rules of behavior prior to account issuance and annually thereafter

Table 3: CMS Defined Parameters - Control PL-4

The following steps detail the CMS process for ensuring that CMS users review and acknowledge the Rules of Behavior.

- **Step 1:** The rules of behavior have been incorporated into the annual Security and Privacy Awareness Training, and all EUA users must take the Computer Based Training (CBT) located at https://www.cms.gov/cbt/forms/isspa.aspx. The training is taken by all EUA users initially prior to account issuance and annually thereafter
- **Step 2:** Each year based on the date of account issuance each user receives an email requiring them to review and complete the annual CBT
- Step 3: Training records are maintained using the CBT database and include the UID and the date the individual last completed the training
- **Step 4:** Use of Social Media/Networking Sites and Posting Organizational Information on Public Websites have been incorporated in the annual Security and Privacy Awareness Training and the RoB is electronically signed as the last step of that training. Failing to complete the CBT training will result in the user having his/her credentials revoked

3.4 Social Media and Networking Restrictions (PL-4(1))

CMS includes in the RoB explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. The rules of behavior have been incorporated into the annual Security and Privacy Awareness Training which is delivered via CBT. See section 3.3 of this document for procedures for completing the CBT.

3.5 Information Security Architecture (PL-8)

This control addresses actions taken by CMS organizations in the design and development of information systems. The CMS information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture. The CMS information security architecture includes:

- Architectural Description
- Placement/Allocation of Security Functionality
- Allocation of Security Controls
- Security-related information for external interfaces, information being exchanged across the interfaces
- Protection mechanisms associated with each interface.

In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs. The table below outlines the CMS organizationally defined parameters (ODPs) for this control.

Control	Control Requirement		CMS Parameter	
PL-8	b.	Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture;	b.	As necessary but no less than every three years

Table 4: CMS Defined Parameters – Control PL-8

The CMS TRA articulates the technical architecture of the CMS processing environments. As a foundation document, the CMS TRA is designed to assist all agency business partners in developing to, transitioning to, and maintaining the CMS Processing Environments in accordance with CMS's enterprise technical architecture. The CMS enterprise technical architecture supports five critical technical objectives that enable the agency's healthcare mission:

- Secure the CMS operating environment
- Allow for the efficient allocation of CMS workloads across data centers
- Provide appropriate and sufficient disaster recovery and business continuity capability
- Facilitate the migration and transition of CMS business owner applications into new Processing environments
- Build an enterprise technical architecture that anticipates and responds to CMS's mission and business needs

Appendix A. Acronyms

Selected acronyms used in this document are defined below.

Acronyms	Terms
AO	Authorizing Official
ARS	Acceptable Risk Safeguards
ССВ	Change Control Board
CCIC	CMS Cybersecurity Integration Center
CFACTS	CMS FISMA Controls Tracking System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CMS IS2P2	Information Systems Security and Privacy Policy
CRA	Cyber Risk Advisor
DHS	Department of Homeland Security
EUA	Enterprise User Administration
FEA	Federal Enterprise Architecture
FISMA	Federal Information Security Management Act
ннѕ	Department of Health and Human Services
HHS IS2P	HHS Information System Security and Privacy Policy
HHS-CSIRC	HHS Computer Security Incident Response Center
HHS-PIRT	HHS Privacy Incident Response Team
НІРРА	Health Insurance Portability and Accountability Act of 1996
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
ІТ	Information Technology

Acronyms	Terms
MOU	Memorandum of Understanding
ОМВ	Office of Management and Budget
OpDiv	Operating Division
PL	Planning Control Family
RMH	Risk Management Handbook
RoB	Rules of Behavior
SOP	Senior Official for Privacy
SORN	System of Records Notices
TRA	Technical Reference Architecture
TRB	Technical Review Board
XLC	Expedited Life Cycle

Appendix B. Glossary of Terms

Selected terms and definitions in this document are defined below (e.g. Risk Assessment and a brief definition of its meaning).

Terms	Definitions	
Acceptable Risk Safeguards	CMS Information Security Acceptable Risk Safeguards (ARS), http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity.	
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	
Centers for Medicare & Medicaid Services	CMS covers 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace.	
Change Control Board	Ensures change control processes are being followed in accordance with the system security plan.	
Chief Information Officer	 Agency official responsible for: Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency 	
Chief Information Security Officer	The incumbent in the position entitled Chief Information Security Officer. The CISO ¹⁹ must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 11, <i>OpDiv CISOs</i> . The CISO carries out the CIO's information security responsibilities under federal requirements in conjunction with the SOP.	

¹⁹ Some government directives and standards also refer to this position as the Senior Information Security Officer or Senior Agency Information Security Officer

•

Terms	Definitions
CMS Cybersecurity Integration Center	The CCIC monitors, detects, and isolates information security and privacy incidents and breaches across the CMS enterprise IT environment. The CCIC provides continual situational awareness of the risks associated with CMS data and information systems throughout CMS. The CCIC also provides timely, accurate, and meaningful reporting across the technical, operational, and executive spectrum.
CMS FISMA Controls Tracking System	CMS Data Base that maintains current FISMA information (e.g., POCs, artifacts) to support organizational requirements and processes (e.g., communication, contingency planning, training, data calls)
Cyber Risk Advisor	Acts as Subject Matter Expert in all areas of the CMS Risk Management Framework (RMF).
Department of Health and Human Services	The United States Department of Health and Human Services (HHS), also known as the Health Department, is a cabinet-level department of the U.S. federal government with the goal of protecting the health of all Americans and providing essential human services. Its motto is "Improving the health, safety, and well-being of America." Before the separate federal Department of Education was created in 1979, it was called the Department of Health, Education, and Welfare (HEW).
Department of Homeland Security	The federal government department responsible for the security and protection of American land, territorial waters and people. The DHS was established in response to the terrorist attacks of September 11, 2001 by the Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135 (Nov. 25, 2002))
eXpedited Life Cycle	CMS-XLC-1: The CISO must integrate information security and privacy into the CMS life cycle processes. The XLC provides the processes and practices of the CMS system development life cycle in accordance with the CMS Policy for Information Technology (IT) Investment Management & Governance. The CMS CISO maintains the RMH Volume 1 Chapter 1, Risk Management, in the XLC to document the CMS information system life cycle, in accordance with the RMF.
Federal Enterprise Architecture	A business-based framework developed by OMB to identify opportunities to simplify processes and unify work across the agencies and within the lines of business of the federal government in order to transform the federal government into one that is citizencentered, customer-focused, results-oriented, and market-based and to maximize technology investments to better achieve mission outcomes.
Federal Information Security and Modernization Act	Requires agencies to integrate information technology (IT) security into the capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the OMB

Terms	Definitions
Health Insurance Portability and Accountability Act of 1996	An act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.
HHS Computer Security Incident Response Center	A capability set up for assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).
HHS Privacy Incident Response Team	The FISMA system SOC/IRT may consist of federal employees or contractors and must fulfill all of the FISMA system-level responsibilities identified in the HHS IS2P Appendix A Section 13, OpDiv CSIRT, and applicable responsibilities under the HHS IS2P Appendix A Section 14, HHS PIRT. The FISMA system SOC/IRT reports to the Agency Security Operations, which is responsible for CMS-wide incident management.
Identify Credential and Access Management	A set of capabilities that ensure users must authenticate to information technology resources and have access to only those resources that are required for the job function.
Information System Security Officer	Person responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with System Security Officer (SSO)
	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.
Information Systems Security and Privacy Policy	This Policy provides direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems or systems maintained on behalf of CMS to assure the confidentiality, integrity, and availability of CMS information and systems. As the federal agency responsible for administering the Medicare, Medicaid, Children's Health Insurance Program (CHIP), and Health Insurance Marketplace (HIM); CMS collects, creates, uses, discloses, maintains, and stores personal, healthcare, and other sensitive information ²⁰ subject to federal law, regulation, and guidance

This Policy uses the term "CMS Sensitive Information" as defined in the Risk Management Handbook Volume I Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms (http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-

<u>Technology/InformationSecurity/Downloads/RMH_VI_10_Terms_Defs_Acronyms.pdf</u>) and subject to Executive Order 13556, Controlled Unclassified Information (https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information). This definition includes all data that

Terms	Definitions
Information Technology	The term information technology with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Interconnection Security Agreement	The purpose of this Interconnection Security Agreement (ISA) is to establish procedures for mutual cooperation and coordination between the Centers for Medicare & Medicaid Services (CMS) and other organizations.
Memorandum of Understanding	This document details the agreement between CMS and its organizations regarding the principles under which the initiative will be implemented and operated. It also outlines the activities which CMS and its organizations agree to conduct in preparation for planned implementation of the initiative.

require protection due to the risk and magnitude of loss or harm, such as Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI).

Terms	Definitions
Office of Management and Budget	The Office of Management and Budget (OMB) designated the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) as authorities to provide guidance to federal agencies for implementing information security and privacy laws and regulations, including FISMA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974 ("Privacy Act"). This Policy addresses CMS applicable information security and privacy requirements arising from federal legislation, mandates, directives, executive orders, and Department of Health and Human Services (HHS) policy by integrating NIST SP-800-53v4, Security and Privacy Controls for Federal Information Systems and Organizations, with the Department of Health and Human Services Information Systems Security and Privacy Policy (IS2P) and specific programmatic legislation and CMS regulations. Appendix B lists these authoritative references.
Planning Control Family	The Planning family of controls to ensure information security and privacy planning for FISMA systems are performed within the CMS enterprise environment and on any systems storing, processing, or transmitting CMS information on behalf of CMS.
Protected Health Information	 Individually identifiable health information that is: Transmitted by electronic media, Maintained in electronic media, or Transmitted or maintained in any other form or medium. [HIPAA] Note: PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer.
Risk Management Handbook	The Risk Management Handbook (RMH) compiles CMS standards, requirements, directives, practices, and procedures for protecting CMS information and information systems.
Rules of Behavior	 Guidelines describing permitted actions by users and the responsibilities when utilizing a computer system. The rules that have been established and implemented concerning use of, security in and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment, and limitation of system privileges, and individual accountability.
Senior Official for Privacy	The SOP must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 15, <i>OpDiv SOP</i> . The SOP carries out the CIO's privacy responsibilities under federal requirements in conjunction with the CISO.

Terms	Definitions
System of Records Notices	The Privacy Act mandates the publishing of system of records notices (SORNs) for newly created and revised systems of records. Since its enactment, Office of Management and Budget (OMB) memoranda have provided additional guidance on the interpretation of the Privacy Act.
Technical Reference Architecture	The CMS Technical Reference Architecture provides the authoritative technical architecture approach and technical reference standards for the CMS enterprise. The CMS TRA consists of this foundation document and the CMS TRA Supplements. This foundation document is authorized and approved by the CMS Chief Technology Officer. In conjunction with the TRA, the CMS Technical Review Board (TRB) contributes to the agency's Information Technology (IT) success in three distinct but related roles: Strategy, Guidance, and Execution. The TRB provides technical intellectual continuity of high level architectural decisions and direction. These decisions are documented and communicated in the Technical Reference Architecture (TRA) and its supplements, which are maintained by the TRB.
Technical Review Board	The TRB provides oversight to ensure IT investments are consistent with CMS's IT strategy. The board manages updates to the TRA to promote the CMS IT strategy and assists projects by ensuring solutions are technically sound and on track to deliver promised capabilities on time and on budget.

Appendix C. Applicable Laws and Guidance

Appendix C provides references to both authoritative and guidance documentation supporting the "document". Subsections are organized to "level of authority" (e.g., Statues take precedence over Federal Directives and Policies). The number on each reference represents a mapping which uniquely identifies the reference within the main body of the document.

C.1 Statutes

The Privacy Act of 1974, as amended (5 U.S.C. 552a)

- 1 <u>http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/PrivacyActof1974.html</u>
- Federal Information Security Modernization Act (FISMA) of 2014
 - https://www.congress.gov/bill/113th-congress/senate-bill/2521
 - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- 3 http://www.hhs.gov/hipaa/index.html

C.2 Federal Directives and Policies

- E-Government Act of 2002 (Pub. L. No. 107-347) § 208 http://www.nist.gov/director/oism/upload/PL107-347.pdf
- 2 Code: 5 U.S.C. §552a(e)(10)
 - $\frac{http://www.gpo.gov/fdsys/granule/USCODE-2010-title5/USCODE-2010-title5-partI-chap5-subchapII-sec552a/content-detail.html}{}$
- 3 FedRAMP Rev. 4 Baseline
 - $\frac{https://www.fedramp.gov/files/2015/03/FedRAMP-Control-Quick-Guide-Rev4-FINAL-01052015.pdf}{}$

C.3 OMB Policy and Memoranda

- OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB Memorandum M-03-22)
 - http://www.whitehouse.gov/omb/memoranda m03-22/

- OMB Circular A-130 Management of Federal Information Resources http://www.whitehouse.gov/omb/circulars_a130_a130trans4/
- 3 OMB M-07-16 Memorandum For The Heads of Executive Department and Agencies https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

C.4 NIST Guidance and Federal Information Processing Standards

- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
- NIST SP 800-37 *Guide for Applying the risk Management Framework to Federal Information Systems*http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- NIST SP 800-53-r4 Security and Privacy Controls for Federal Information Systems and Organizations

 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- 4 NIST SP 800 53A-r4 Guide for Assessing the Security Controls in Federal Information Systems

 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf
- NIST SP 800-40-r3, *Guide to Enterprise Patch Management Technologies*http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf
- 6 NIST SP 800-70 r3 National Checklist Program for IT Products Guidelines for Checklist Users and Developers

 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r3.pdf
- 7 FIPS-199 Standards for Security Categorization of Federal Information and Information Systems

 http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- 8 NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

C.5 HHS Policy

- 1 HHS-OCIO-2013-0004 HHS Policy for Personal Use of Information Technology Resources
 - http://www.hhs.gov/ocio/policy/pol-pers-use-it-resources.html (Intranet Only)
- 2 HHS-OCIO-2014-0001 HHS Information System Security and Privacy Policy (HHS IS2P)
 - HHS Information Security and Privacy Policy (IS2P) 2014 Edition. If you are having a problem obtaining a copy of this document, please email fisma@hhs.gov
- 3 HHS- OCIO 2013-0003S HHS Rules of Behavior for Use of HHS Information Resources http://www.hhs.gov/ocio/policy/hhs-rob.html (Intranet Only)
- 4 HHS The Office of the Assistant Secretary for Financial Resources (ASFR)

 http://www.hhs.gov/about/agencies/asfr/ (Intranet Only)
- 5 HHS Office of Grants and Acquisition Policy and Accountability (OGAPA)
 http://www.hhs.gov/about/agencies/asfr/ogapa/

C.6 CMS Policy and Directives

- 1 CMS Information Systems Security and Privacy Policy (IS2P2)

 https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/
- 2 CMS Information Security Acceptable Risk Safeguards (ARS)

 https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html
- 3 CMS Office of Acquisition and Grants Management (OAGM) https://www.cms.gov/About-CMS/Leadership/oagm/
- 4 Risk Management Handbook Volume II Procedure 1.1 Accessing the CFACTS

 https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VII_1-1_Accessing_CFACTS.pdf
- 5 RMH CMS Information Security (IS) Authorization To Operate Package Guide

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ATO_Package_Guide.pdf

6 RMH Risk Management Handbook Volume III Standard 6.2 Plan of Action and Milestones Process Guide

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_6-2_Plan_of_Action_and_Milestones_Process_Guide.pdf

C.7 Associated CMS Resources

- 1 HHS Departmental Security Policy and Standard Waiver Form http://intranet.hhs.gov/it/cybersecurity/policies/index.html (Accessible via intranet only)
- 2 CMS Policy for Acceptable Use of CMS Desktop/Laptop and Other IT Resources https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/Policy-CMS-Policy-for-the-Acceptable-Use-of-CMS-Desktop-Laptop-and-Other-IT-Resources.html
- 3 Risk Management Handbook Volume II Procedure 3.3-Common Control Identification https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VII_3-3_Common_Control_Identification.pdf
- 4 CMS Technical Reference Architecture Version 3.0 February 12, 2013

 https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-CMS-Technical-Reference-Architecture-TRA-.html
- 5 CMS Technical Reference Architecture Application Development Guidelines Supplement Version 1.0 May 13, 2015

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Application-Development-Guidelines.html

6 Technical Review Board Charter Version: 3.0 Last Modified: September 5, 2014 http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/TRBCharter.pdf 7 Centers for Medicare & Medicaid Services (CMS) Information Security (IS) Authorization To Operate Package Guide for more information on ATO Packages.

 $\underline{Systems/CMS\text{-}Information\text{-}Technology/InformationSecurity/downloads/ATO}\\ \underline{Package_Guide.pdf}$

Appendix D. Feedback and Questions

Information Security and Privacy is a dynamic field and as such policies, standards, and procedures must be continually refined and updated. Feedback from the user community is invaluable and ensures that high quality documents are produced and that those documents add value to the CMS community. Should you have any recommendations for improvements to this document please email the CISO mailbox at CISO@cms.hhs.gov. Your feedback will be evaluated for incorporation into future releases of the document. Questions about any of the material included within this document may also be sent to the CISO mailbox.

Appendix E. ARS Standards – Planning (PL)

Control Number	Baseline	Control Name	CMS Control Privacy Controls		CSP/FedRAMP Control
PL-01	High Moderate Low	Security Planning Policy and Procedures	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates (as necessary) the current: 1. Security planning policy within every three (3) years; and 2. Security planning procedures within every three (3) years.		

Control Number	Baseline	Control Name	CMS Control Privacy Controls		CSP/FedRAMP Control
PL-02	High Moderate Low	System Security Plan	The organization: a. Develops a security plan for the information system that is consistent with the Risk Management Handbook (RMH) Procedures; and 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan	The system security plan (SSP) must provide the security category and the PII confidentiality impact level of the system (as described in NIST SP 800-122), describe relationships with, and data flows of, PII to other systems, provides an overview of security and privacy requirements for the system, including the security controls within the Privacy Overlays. The SSP must define the boundary within the system where PII is stored, processed, and/or maintained. The person responsible for meeting information system privacy requirements must provide input to the SSP. IMPLEMENTATION STANDARD(S) Std.1 - (For PHI only) Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)	The SSP must address gaps between the FedRAMP baseline and the ARS required baseline.

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to stakeholders; c. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and d. Updates the plan, minimally every three (3) years, to address current conditions or whenever: - There are significant changes to the information system/environment of operation that affect security; - Problems are identified during plan implementation or security control assessments; - When the data sensitivity level increases; - After a serious security violation due to changes in the threat environment; or - Before the previous security authorization expires; and e. Protects the security plan from unauthorized disclosure and modification.		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
PL- 02(03)	High Moderate	Plan/Coordinate with Other Organizational Entities	The organization plans and coordinates security-related activities affecting the information system with affected internal or external stakeholders, groups, or organizations before conducting such activities in order to reduce the impact on other organizational entities.		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
PL-04	High Moderate Low	Rules of Behavior	The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe the responsibilities and expected behavior with regard to information and information system usage; b. Receives an acknowledgment (paper or electronic) from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior every three (3) years; and d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and reacknowledge when the rules of behavior are revised/updated. e. Informs employees and contractors that the use of CMS information resources for anything other than authorized purposes set forth in the HHS RoB and Policy for Personal Use of Information Technology Resources is a violation of either or both of those policies, and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment. f. Informs employees and	Pursuant to OMB M-07- 16, organizational rules of behavior must include a policy outlining the rules of behavior to safeguard personally identifiable information (PII) and identifying consequences and corrective actions for failure to follow these rules. Consequences should be commensurate with level of responsibility and type of PII involved.	

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			contractors that the use of CMS information resources is subject to the HHS Policy for Monitoring Employee Use of HHS IT Resources; g. In addition to the HHS directive, the organization may define a system-level RoB acknowledgement.		
PL- 04(01)	High Moderate	Social Media and Networking Restrictions	The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
PL-08	High Moderate	Information Security Architecture	The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates (as necessary) the information security architecture no less often than every three (3) years and whenever changes are made to the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions. d. Ensures that the planned information security architecture is consistent with the CMS's enterprise architecture program and is based on the taxonomy of the Federal Enterprise Architecture (FEA).		

Appendix F. Control/Policy Cross Reference Table

NIST 800-53r4 PL Controls	CMS ARS PL Control	CMS IS2P2 Policy	HHS IS2P Policy
PL-1 Security Planning Policy and Procedures	PL-1 Security Planning Policy and Procedures	PL-1, PL-1.1, PL-1.2	PL-1 Security Planning Policy and Procedures
PL-2 System Security Plan	PL-2 System Security Plan	PL-1.1.1.1, PL-1.1.1.2,	PL-2 System Security Plan
PL-2(1) System Security Plan Concept of Operations	Not Selected	Not Selected	Not Selected
PL-2(2) System Security Plan Functional Architecture	Not Selected	Not Selected	Not Selected
PL-2(3) Security Plan Plan/Coordinate with Other Organizational Entities	PL-02(03) Plan/Coordinate with Other Organizational Entities *	PL-1.1.1.3, PL-1.1.4, PL-1.1.4.1	PL-2 c.e.3 Plan/Coordinate with Other organizational Entities
PL-3 System Security Plan Update: This control has been withdrawn	Not Selected	Not Selected	Not Selected
PL-4 Rules of Behavior	PL-4 Rules of Behavior	PL-1.1.4.2, PL-1.1.4.2.1, PL- 1.1.4.2.3, PL-1.1.4.3	PL-4 Rules of Behavior
PL-4(1) Rules of Behavior Social Media and Networking Restrictions	PI-04(01) Social Media and Networking *	PL-1.1.4.2.2	PL-4 c.e.1 Social Media and Networking Restrictions
PL-5 Privacy Impact Assessment: This control has been withdrawn	Not Selected	Not Selected	Not Selected
PL-6 Security Related Activity Planning: This control has been withdrawn	Not Selected	Not Selected	Not Selected
PL-7 Security Concept of Operations	Not Selected	Not Selected	Not Selected
PL-8 Information Security Architecture	PL-8 Information Security Architecture	PL-1.1.2, PL-1.1.2.1, PL-1.1.2.2, PL-1.1.2.3, PL-1.1.3,	PL-8 Information Security Architecture
PL-8(1) Information Security Architecture Defense in Depth	Not Selected	Not Selected	Not Selected

NIST 800-53r4 PL Controls	CMS ARS PL Control	CMS IS2P2 Policy	HHS IS2P Policy
PL-8(2) Information Security Architecture Supplier Diversity	Not Selected	Not Selected	Not Selected
PL-9 Central Management	Not Selected	Not Selected	Not Selected