Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Risk Management Handbook (RMH) Chapter 04: Security Assessment and Authorization (CA)

Final

Version 1.1

December 07, 2020

Record of Changes

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

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
0.1	09/08/2017	All	ISPG	Initial Draft
0.2	10/10/2017	All	ISPG	First Review
0.3	01/25/2018	All	ISPG	OIT Review
0.4	03/09/2018	Section 3.3	ISPG	Alignment with new HHS POAM Guidance
0.5	04/04/2018	All	ISPG	SWIFT Review
0.6	08/23/2018	All	ISPG	Updated with new RMH template; updated to include most recent CA-related findings and weaknesses
1.0	01/09/2019	All	ISPG	Publication
1.1	12/07/2020	Section 6.4	ISPG	Updated CCIC email address

Effective Date/Approval

This Procedure becomes effective on the date that CMS's Deputy Chief Information Security Officer signs it and remains in effect until it is rescinded, modified or superseded.

Signature: /S/ Date of Issuance

Michael Pagels
Director, Division of Security and
Privacy Policy and Oversight (DSPPO)
and Senior Official for Privacy

Table of Contents

Tables

Figures

1. Introduction

1.1 Purpose

The Centers for Medicare & Medicaid Services (CMS) Risk Management Handbook (RMH) Chapter 4 Security Assessment and Authorization provides the procedures for implementing the requirements of the CMS Information Systems Security and Privacy Policy (IS2P2) and the CMS Acceptable Risk Safeguards (ARS). The following is a diagram that breaks down the hierarchy of the IS2P2, ARS, and RMH:

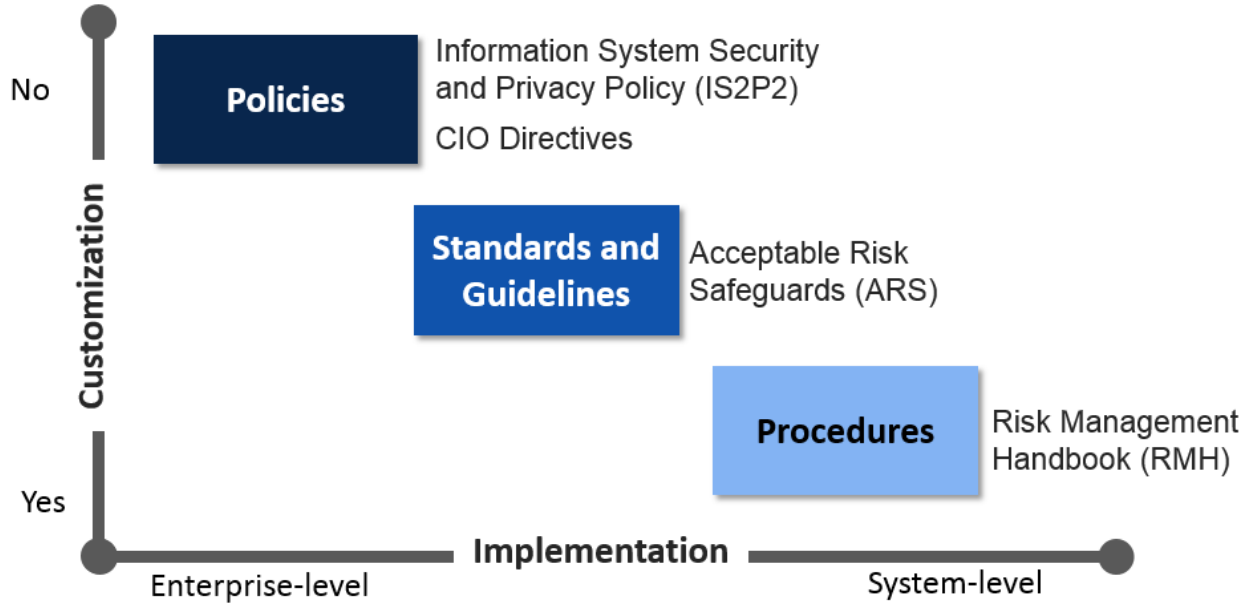

Figure 1: Three-Tiered Hierarchy

This document describes procedures that facilitate the implementation of security controls associated with the Security Assessment and Authorization (CA) family of controls. To promote consistency among all RMH Chapters, CMS intends for Chapter 4 to align with guidance from the National Institute of Standards and Technology (NIST). CMS incorporates the content of NIST's Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, into its governance documents, tailoring that content to the CMS environment.

1.2 Authority

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor. The Federal Information Security Modernization Act of 2014 designates NIST with responsibility to develop guidance to federal agencies on information security and privacy requirements for federal information systems.

As an operating division of the Department of Health and Human Services (HHS), CMS must also comply with the HHS IS2P, Privacy Act of 1974 ("Privacy Act"), the Privacy and Security Rules developed pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the E-Government Act of 2002, which relates specifically to electronic authentication requirements. The HHS Office for Civil Rights (OCR) is responsible for enforcement of the HIPAA Security and Privacy Rules. CMS seeks to comply with the requirements of these authorities, and to specify how CMS implements compliance in the CMS IS2P2.

HHS and CMS governance documents establish roles and responsibilities for addressing privacy and security requirements. In compliance with the 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 program. HHS also designates the CMS Senior Official for Privacy (SOP) as the CMS authority for implementing the CMS-wide privacy program. Through their authority given by HHS, the CIO and 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 support the policies and the procedures referenced in this handbook to ensure compliance with federal requirements for implementation of information security and privacy controls.

1.3 Scope

This handbook documents procedures that facilitate the implementation of the privacy and security controls defined in the CMS IS2P2 and the CMS ARS. This RMH Chapter provides authoritative guidance on matters related to the Security Assessment and Authorization family of controls for use by CMS employees and contractors that support the development, operations, maintenance, and disposal of CMS information systems. This handbook does not supersede any applicable laws, existing labor management agreements, and/or higher-level agency directives or other governance documents.

1.4 Background

This handbook aligns with NIST SP 800-53 catalogue of controls, the CMS IS2P2, and the CMS ARS. Each procedure relates to a specific NIST security control family. Additional sections of this document crosswalk requirements to other control families and address specific audit requirements issued by various sources (e.g., OMB, OIG, HHS, etc.).

RMH Chapter 4 provides processes and procedures to assist with the consistent implementation of the CA family of controls for any system that stores, processes, or transmits CMS information on behalf of CMS. This chapter identifies the policies, minimum standards, and procedures for the effective implementation of selected security and privacy controls and control enhancements in the CA family.

CMS's comprehensive information security and privacy policy framework includes:

- An overarching policy (CMS IS2P2) that provides the foundation for the security and privacy principles and establishes the enforcement of rules that will govern the program and form the basis of the risk management framework
- Standards and guidelines (CMS ARS) that address specific information security and privacy requirements
- Procedures (RMH series) that assist in the implementation of the required security and privacy controls based upon the CMS ARS standards.

FISMA further emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a risk-defined frequency. NIST SP 800-53 states under the CA control family that an organization must define, develop, disseminate, review, and update its Security Assessment and Authorization documentation at least once every three years. See the required review frequencies for any particular security artifact as specified with the CMS ARS. This includes a formal, documented system security package that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented processes and procedures to facilitate the implementation of the Security Assessment and Authorization policy and associated controls.

The Security Assessment and Authorization process exists within the Risk Management Framework (RMF) which emphasizes:

- Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls
- Maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes
- Providing essential information to senior leaders to facilitate decisions regarding the mitigation or acceptance of information-systems-related risk to organizational operations and assets, individuals, external organizations, and the Nation.

The RMF[1] has the following characteristics:

- Promotes the concept of near-real-time risk management and ongoing-information-system authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security and privacy protections into the enterprise architecture and eXpedited Life Cycle (XLC);
- Provides guidance on the selection, implementation, assessment, and monitoring of controls and the authorization of information systems;
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and

[1] https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

- Establishes responsibility and accountability for security and privacy controls deployed within organizational information systems and inherited by those systems (i.e., common controls)

2. Policy

Policy delineates the security management structure, clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress, compliance, and 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 information systems.

2.1 Information Systems Security and Privacy Policy (IS2P2)

The CMS IS2P2[2] defines the framework and policy under which CMS protects and controls access to CMS information and information systems in compliance with HHS policy, federal law, and regulations. This Policy requires all CMS stakeholders to implement adequate information security and privacy safeguards to protect all CMS sensitive information.

The policy contained within the CMS IS2P2 and the procedures contained within this document assist in satisfying the requirements for controls that require CMS to create a policy and associated procedures related to Security Assessment and Authorization for information systems.

2.2 Chief Information Officer (CIO) Directives

The CMS Chief Information Officer (CIO), the CMS Chief Information Security Officer (CISO), and the CMS Senior Official for Privacy (SOP) jointly develop and maintain the CMS IS2P2. The CIO delegates authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy Program as appropriate.

The dynamic nature of information security and privacy disciplines and the constant need for assessing risk across the CMS environment can cause gaps in policy, to arise outside of the policy review cycle. The CMS Policy Framework includes the option to issue a CIO Directive[3] to address identified gaps in CMS policy and instruction to provide immediate guidance to CMS stakeholders while a policy is being developed, updated, cleared, and approved.

3. Standards

Standards define both functional and assurance requirements within the CMS security and privacy environment. CMS policy is executed with the objective of enabling consistency across the CMS environment. The CMS environment includes users, networks, devices, all software, processes,

[2] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Systems-Security-and-Privacy-Policy-IS2P2.html?DLPage=1&DLEntries=10&DLFilter=is2&DLSort=0&DLSortDir=ascending

[3] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/Policies.html

information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. These components are responsible for meeting and complying with the security and privacy baseline defined in policy and further prescribed in standards. The parameters and thresholds for policy implementation are built into the CMS standards, and provide a foundation for the procedural guidance provided by the Risk Management Handbook series.

3.1 Acceptable Risk Safeguards (ARS)

The CMS Acceptable Risk Safeguards (ARS)[4] provides guidance to CMS and its contractors as to the minimum acceptable level of required security and privacy controls that must be implemented to protect CMS's information and information systems, including CMS sensitive information. The initial selection of the appropriate controls is based on control baselines. The initial control baseline is the minimum list of controls required for safeguarding an IT system based on the organizationally identified needs for confidentiality, integrity, and/or availability.

A different baseline exists for each security category (high, moderate, low) as defined by NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. The ARS provides a catalog of low, moderate, and high controls, in addition to non-mandatory controls outside of the FIPS-199 baseline selection. The ARS, based upon the FIPS 200 and NIST SP 800-53, provides guidance on tailoring controls and enhancements for specific types of missions and business functions, technologies, or environments of operation. Users of the ARS may tailor specific mandatory controls as well as most of the non-mandatory and unselected controls.

4. HIPAA Integration

The HIPAA Security Rule is designed to be flexible, scalable, and technology-neutral, which enables it to be adaptive and seamlessly integrate with detailed frameworks such as FISMA. Though both regulations are governed by different federal agencies, the HIPAA Security Rule only applies to covered entities and their business associates as defined within HIPAA. Implementation of the FISMA requirements helps achieve compliance with the HIPAA Security Rule. HIPAA provides guidance to address the provisions required for the security of health-related information, whereas FISMA presents instructions for the security of the information and the information systems that support these activities.

The following table is a crosswalk of what controls found in this RMH map to specific sections and requirements found in HIPAA.

Security Assessment and Authorization (CA) Control	HIPAA Section
Security Assessments (CA-2)	§164.308(a)(1)(ii)(A); §164.308(a)(7)(ii)(E); §164.308(a)(8); §164.310(a)(1);

[4] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending

	§164.312(a)(1); §164.316(b)(2)(iii); §164.306(e); §164.308(a)(7)(ii)(D); §164.308(a)(2); §164.308(a)(3)(ii)(A); §164.308(a)(3)(ii)(B); §164.308(a)(4); §164.310(a)(2)(iii); §164.312(a)(2)(ii); §164.308(a)(1)(i); §164.308(a)(6)(ii); §164.314(a)(2)(i)(C); §164.314(a)(2)(iii); §164.308(a)(5)(ii)(B); §164.308(a)(5)(ii)(C)
System Interconnections (CA-3)	§164.308(a)(1)(ii)(A); §164.308(a)(3)(ii)(A), §164.308(a)(8); §164.310(d); §164.308(a)(1)(ii)(D), §164.312(b)
Continuous Monitoring (CA-7)	§164.308(a)(1)(ii)(A); §164.308(a)(7)(ii)(E); §164.308(a)(8); §164.310(a)(1); §164.312(a)(1); §164.316(b)(2)(iii); §164.306(e); §164.308(a)(7)(ii)(D); §164.308(a)(6)(ii); §164.308(6)(i); §164.308(a)(1)(ii)(D); §164.308(a)(5)(ii)(B); §164.308(a)(5)(ii)(C); §164.310(d)(2)(iii); §164.312(b); §164.314(a)(2)(i)(C); §164.314(a)(2)(iii); §164.312(e)(2)(i); §164.310(a)(2)(ii); §164.310(a)(2)(iii); §164.308(a)(3)(ii)(A); §164.312(a)(2)(i); §164.312(d); §164.312(e); §164.310(b); §164.310(c); §164.310(d)(1); §164.314(b)(2)(i); §164.308(a)(2); §164.308(a)(3)(ii)(B); §164.308(a)(4); §164.312(a)(2)(ii); §164.308(a)(1)(i); §164.308(a)(1)(ii)(B)
Penetration Testing (CA-8)	§164.308(a)(1)(ii)(A); §164.308(a)(7)(ii)(E); §164.308(a)(8); §164.310(a)(1); §164.312(a)(1); §164.316(b)(2)(iii)
Internal System Connections (CA-9)	§164.308(a)(1)(ii)(A); §164.308(a)(3)(ii)(A); §164.308(a)(8); §164.310(d)

5. Roles and Responsibilities

A comprehensive list of information security and privacy roles and responsibilities for CMS stakeholders is contained in the CMS IS2P2. The following roles from the CMS IS2P2 are specific to the procedures contained within this RMH chapter.

Roles	Applicable Controls
HHS Chief Information Officer (CIO)	NA
HHS Chief Information Security Officer (CISO)	NA
CMS Chief Information Officer (CIO)	CA-6; CA-9
CMS Chief Information Security Officer (CISO)	CA-2; CA-2(1); CA-5; CA-6
CMS Information System Security Officer (ISSO)	CA-2; CA-2(1); CA-3; CA-5; CA-6; CA-8
CMS Cyber Risk Advisor (CRA)	CA-2;CA-2(1); CA-3; CA-5; CA-6, CA-8
CMS Senior Official for Privacy (SOP)	NA
CMS Privacy SME	NA
CMS Business Owner (BO)	CA-2; CA-2(1);CA-3; CA-6; CA-8
CMS Federal Employee and Contractors	CA-5; CA-6; CA-8
CMS Data Guardian	NA
CMS System Owner	CA-2; CA-3; CA-3(5); CA-5; CA-6; CA-9

6. Procedures

This section contains the applicable procedures that facilitate the implementation of the CA family security controls as required by NIST 800-53, CMS IS2P2, and CMS ARS. To increase traceability, each procedure maps to the associated NIST controls using the control number from the CMS IS2P2.

6.1 Security Assessments (CA-2)

CMS must assess security and privacy controls in CMS information systems and the environments in which those systems operate to determine if the controls are implemented appropriately, operating as intended, and producing the desired results. The output from a security controls assessment provides essential information to the CMS Authorizing Official (AO) needed to make risk-based decisions in support of the security authorization process. The scope of a security assessment is documented in a Security Assessment Plan (SAP), which identifies the security controls and enhancements under assessment, describes the assessment procedures utilized to determine the security control effectiveness, and outlines the assessment environment, team, and roles and responsibilities. The result of the security assessment is documented in a Security Assessment Report (SAR), which is provided to the CMS AO.

Some items that would require a security assessment include:

- Significant change that affects the security state of the information system
- Required frequency depending on control and system categorization
- ATO schedule (once every three years)
- Reassessment of selected controls

The table below outlines the CMS Organizationally Defined Parameters (ODPs) for CA-2:

Table 1: CMS Defined Parameters – Control CA-2

Control	Control Requirement	CMS Parameter
CA-2	The organization: b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles]	b. Assesses the security and privacy controls in the information system and its environment of operation, as defined in implementation standards, within every three hundred sixty-five (365) days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; d. Provides the results of the security and privacy control assessment within thirty (30) days after its completion, in writing, to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system

Planning, execution and reporting are the three phases of a security assessment. The following steps outline the process for conducting a security assessment on CMS information systems:

Phase I: Planning

- **Step 1:** The ISSO provides a copy of the current System Security Plan (SSP) and any additional information related to the information system boundary (e.g. hardware/software listing, High Level Architecture (HLA) Diagrams, Data Flow Diagrams, etc.) that is not contained in the SSP to the independent assessor.

- **Step 2:** The independent assessor reviews the SSP and additional information provided by the ISSO and drafts a SAP. A template for a SAP is provided in Appendix D. Independent assessors may utilize their own template as long as it captures all of the elements identified in the CMS template. The independent assessor provides a copy of the draft SAP to the ISSO for review and comment.
- **Step 3:** The ISSO reviews the draft SAP, briefs/consults the BO as needed, and provides comments to the independent assessor.
- **Step 4:** The independent assessor updates the plan to address the comments received from the ISSO and returns the plan to the ISSO for approval.
- **Step 5:** The ISSO confirms all required updates to the SAP and presents the SAP to the BO for approval.
- **Step 6:** The BO or BO Representative such as the System Developer Maintainer (SDM) approves the SAP.

Phase II: Execution

- **Step 1:** With an approved SAP, the independent assessor conducts a kickoff meeting to brief the assessment stakeholders on the assessment approach, logistics, and schedule.
- **Step 2:** The independent assessor executes the assessment procedures contained within the SAP using three methods: interview, examine, and test.
    - **Interview –** conducted with relevant information system stakeholders to confirm the security control implementations as documented in the SSP.
    - **Examine –** documentation and artifacts are provided to the independent assessor demonstrating the implementation of the security controls as documented in the SSP.
    - **Test** – manual tests are executed and/or automated tools (e.g. vulnerability scans, penetration tests, DISA STIG outputs, etc) are utilized to evaluate the effectiveness of the implemented security controls.
      The ISSO and relevant stakeholders support the assessment activities by responding to the requests of the independent assessor, which may consist of requests for interview, artifacts/documentation, or access to the system for technical testing.
- **Step 3:** At the conclusion of the assessment activities, the independent assessor conducts an assessment out-brief with the relevant stakeholder to review the results of the assessment, discuss assessment findings, and present recommendations.

Phase III: Reporting

- **Step 1:** Following the assessment out-brief, the independent assessor drafts the Security Assessment Report (SAR) that contains the comprehensive results of the assessment (i.e. controls satisfied or other than satisfied). A template for the SAR is located in Appendix E. Independent assessors may utilize their own template as long as it captures all of the elements identified in the CMS template.
- **Step 2:** The ISSO reviews and forwards the SAR to all relevant stakeholders requesting feedback. Included in the SAR are findings and the corresponding risk levels (High, Moderate, Low) with recommended actions to mitigate the risks. It is important that the ISSO and relevant stakeholders review and analyze these risks in determining corrective actions and mitigation plans. The ISSO compiles all of the feedback into a single document and submits the comprehensive feedback to the independent assessor.

- **Step 3:** The independent assessor updates the SAR to address the feedback received from CMS and provides the updated SAR to the ISSO for acceptance.
- **Step 4:** The ISSO confirms the updates to the SAR and briefs the CMS BO. With the acceptance of the BO, the SAR is considered an accepted deliverable. The ISSO uploads the final SAR to the CMS FISMA Controls Tracking System (CFACTS) tool. It is important to remember that the loading of weaknesses into CFACTS shall be done in a timely manner as these weaknesses are considered time sensitive.
- **Step 5:** With the approved SAR, the independent assessor creates a CMS Assessment and Audit Tracking (CAAT) spreadsheet that will facilitate the upload of the assessment results into the CFACTS tool. A template for the CAAT spreadsheet is located in Appendix H. Once completed, the independent assessor emails the CAAT spreadsheet to the CISO mailbox at CISO@cms.hhs.gov copying the CMS ISSO.

6.1.1 Security Assessments | Independent Assessors (CA-2(1))

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. At CMS, the CISO defines the required level of independence of the assessor.

CMS must also engage independent third-party assessors when conducting security assessments on High Value Assets (HVAs). These assessments must include a Risk and Vulnerability Assessment (RVA) and a Security Assessment Report (SAR).

The table below outlines the CMS ODPs for CA-2(1):

Table 2: CMS Defined Parameters – Control CA-2(1)

Control	Control Requirement	CMS Parameter
CA-2(1)	The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.	The organization employs assessors or assessment teams with CMS CISO defined level of independence to conduct security control assessments.

The CISO currently maintains a contract with an independent third party assessor that is available for use by BOs and ISSOs to fulfill the independent security assessment requirement. The steps below outline the process for utilizing that contract:

- **Step 1:** The ISSO notifies the CRA that an assessment is being requested. A tentative date for the assessment to begin should be provided.

- **Step 2:** The CRA provides the ISSO with the current pricing for the assessment and instructions for using the Comprehensive Acquisitions Management System (CAMS) and notifies the independent assessor that an assessment needs to be scheduled.
- **Step 3:** At least six weeks prior to the assessment kick-off, the ISSO must work with the BO to move funds for the assessment using the CAMS.
- **Step 4:** The assessment may begin once the funds are verified as available via the CAMS.

6.1.2 Security Assessments | Specialized Assessments (CA-2(2))

In today's dynamic threat environment, preparation is critical to responding to ever-evolving cyber threats. One of the ways to prepare for cyber events is to conduct specialized security assessments (e.g. insider threat assessments, malicious user testing, information system monitoring). These assessments can be utilized to assess the current capabilities of the organization and identify areas for improvement. Special security assessments designed to focus on current threats based on an assessment of risk.

The table below outlines the CMS ODPs for CA-2(2):

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

Control	Control Requirement	CMS Parameter
CA-2(2)	The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing	The organization includes as part of security control assessments, within every three hundred sixty-five (365) days, announced or unannounced in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; and performance/load testing.

6.1.3 Security Assessments | External Organizations (CA-2(3))

The independent assessment of CMS information systems is critical to achieving impartiality and avoiding conflicts of interest in evaluating the implementation of a security control baseline. Since assessments are conducted on a recurring schedule dependent upon audits and the Assessment & Authorization (A&A) process, utilizing previous assessment results, compliance descriptions, and findings may seem like an efficient way to conduct full security control assessments. However, the benefit of deduction in time and resource consumption with the reused assessment documentation subtracts from the overall quality of the test result write-ups and the accuracy of risk identification. To avoid this risk, the security control enhancement specifies that a high system must contract out assessment related work to an external organization, such as a Third Party Assessment Organization (3PAO).The experience and capability of a 3PAO can vary depending on their past work completed with other organizations. By utilizing a 3PAO to conduct an

assessment, the full assessment will rely on an independent and refreshed viewing and testing of implemented security controls.

6.2 System Interconnections (CA-3)

This control covers the authorization, documentation, and review of connections between information systems known as system interconnections. For CMS information systems in different organizations, or external to the federal organization (i.e. private sector), an Interconnection Security Agreement (ISA) must be signed by both parties.

In addition, system connections between federal and non-federal organizations should include contractual agreements. Interconnections where information systems are within the same organization, or share the same authorizing official, an ISA is not required and instead will document the interface characteristics of the information system within their respective security plans. The type of data agreement needed is dependent on several factors and further guidance on using data agreements is found in Appendix J.

The table below outlines the CMS ODPs for system interconnections:

Table 4: CMS Defined Parameters – Control CA-3

Control	Control Requirement	CMS Parameter
CA-3	The organization: c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].	The organization: c. Reviews and updates the interconnection agreements no less than once every year and whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement as a verification of enforcement of security requirements.

The following steps detail the CMS specific process for authorizing interconnection between information systems:

- **Step 1:** System Owner/BO requests interconnection between his/her information system to another information system through use of an Interconnection Security Agreement (ISA), other comparable agreement such as Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA), Service Level Agreement (SLA), or specific contractual clause, as long as the appropriate interconnection details are included. However, the use of an ISA is highly recommended to reduce liability and risk to the organization and to ensure complete compliance with NIST standards. A template for the ISA is provided in Appendix H. A template for the MOU/MOA is provided in Appendix L.
- **Step 2:** System Owner/BO documents (1) the interface characteristics; (2) the security requirements; and (3) the nature of the information communicated for each

interconnection within the applicable SSP. Internal interconnections are authorized when the ATO memo is signed. If the connection is an external connection, continue to Step 3 and Step 4.

- **Step 3:** ISAs or other comparable agreement shall be reviewed and updated by the System Owner no less than once per year or when significant changes, affecting the security state of the information system, are implemented that impact that validity of the agreement as an effective enforcement of security requirements. The applicable ISSO shall upload the signed ISA to CFACTS, specifically within the Authorization section under Interconnections.
- **Step 4:** System Owner shall only activate a system interconnection including, but not limited to, testing when a signed interconnection is signed and enforceable.

6.2.1 System Interconnections | Connections to Public Networks (CA-3(5))

This control covers the connections between information systems and external networks. External networks connections expose the opportunity for intentional and accidental disclosure of sensitive information. This control shall help CMS constrain information system connectivity to external domains and reduce the organization's exposure to incidents.

The table below outlines the CMS ODPs for connections to public networks:

Table 5: CMS Defined Parameters – Control CA-3(5)

Control	Control Requirement	CMS Parameter
CA-3(5)	The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.	The organization employs, and documents in the applicable system security plan, a deny-all, permit-by-exception, policy for allowing defined information systems (defined in the applicable security plan) to connect to external information systems.

- **Step 1:** Within the SSP, the System Owner defines what information systems are allowed to connect to external information systems and includes a description of the security control employed to mitigate the risk associated with the connection.
- **Step 2:** If a connection is permitted, the System Owner shall employ a deny-all, allow by exception policy. The System Owner shall determine what exceptions, if any, are acceptable.

6.3 Plan of Action and Milestones (CA-5)

The Plan of Action and Milestones (POA&M), prepared for the authorizing official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned:

(i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and risk
(ii) to address the residual vulnerabilities in the information system.

The Plan of Action and Milestones identifies:

(iii) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; and
(iv) the resources required to accomplish the tasks.

At CMS, the ISSO is responsible for maintaining the POA&M on behalf of the information system owner by using the CFACTS tool. The table below outlines the ODPs for the POA&M:

Table 6: CMS Defined Parameters – Control CA-5

Control	Control Requirement	CMS Parameter
CA-5	The organization: a. Develops a plan of action and milestones for the information system 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; and c. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security	The organization: a. Develops and submits a POA&M for the information system within thirty (30) days of the submission of final results (e.g., Final Report) for every internal/external audit/review or test (e.g., Security Control Assessment [SCA], penetration test, automated configuration and vulnerability scan results) 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; and b. Updates and submits existing plan of action and milestones monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

	impact analysis, and continuous monitoring activities.	

At the completion of a security controls assessment, the independent assessor completes a CMS Assessment and Audit Tracking (CAAT) spreadsheet. The CAAT spreadsheet is utilized for all CMS audits, assessments and penetration testing vulnerabilities. The completed CAAT spreadsheet is emailed to the CMS CISO mailbox at CISO@cms.hhs.gov for upload into the CFACTS tool. Once uploaded into CFACTS, the weaknesses are automatically generated for all items with a status of "other than satisfied." The following steps detail the CMS-specific process for creating and maintaining the POA&Ms for the identified weaknesses:

6.3.1 Creating a POA&M

The ISSO for the associated information system receives an automated email notification from the CFACTS tool identifying a new weakness. At CMS, a weakness can be identified from any of a number of sources including, but not limited to:

- HHS Office of Inspector General (OIG) Audits
- Government Accountability Office (GAO) Audits
- Chief Financial Officer (CFO) Reviews
- OMB A-123 Internal Control Reviews
- Annual Assessments
- FISMA Audits
- Security Control Assessments
- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) Section 912
- Audits
- Internal Revenue Service (IRS) Safeguard Reviews
- Department of Homeland Security (DHS) Risk Vulnerability Assessments (RVA)
- DHS Cyber Hygiene
- Penetration Testing
- Vulnerability Scanning

The ISSO has 30 days to create the POA&M within CFACTS. By associating milestones to each weakness using the following steps, the ISSO will create the POA&M:

- **Step 1:** The ISSO or support contractor locates the weaknesses in CFACTS using the subtasks below:
    - Login to CFACTS and select the *"Assessment & Authorization (A&A)"* tab from the top menu
    - Click on "Authorization Package – Records" under the "Quick Links" column and select the appropriate information system from the list. You may also find the information system by clicking *"Search Records"* and specifying search criteria

- Once the information system has been located click on the system name to open the authorization package for the system
- Select the *"Controls"* tab from the top navigation tab of the authorization package
- Scroll down to the *"Allocated Controls"* section to locate the hyperlinks for the POA&Ms associated with the controls with a status of "*Other Than Satisfied"*
- Click the hyperlink for a POA&M to open that POA&M

- **Step 2:** Click the *"Edit"* button to switch to edit mode allowing new milestones to be added. Scroll down to the *"Milestones"* section and click the *"Add New"* link to add a new milestone.
- **Step 3:** Enter a milestone name, milestone description, and select a scheduled completion date. Click the *"Save"* button at the top left corner of the milestones window.

NOTE: The following remediation timelines apply based on the weakness risk level:

- ***High Risks –*** *must be remediated within 30 days of the weakness creation date*
- ***Moderate Risks –*** *must be remediated within 60 days of the weakness creation date*
- ***Low Risks –*** *must be remediated within 365 days of the weakness creation date*

After 90 days from the weakness creation date the POA&M will automatically be changed to a status of "Ongoing" this will lock the milestones removing the ability to edit them. For this reason, the ISSO must complete the entire POA&M entry as soon as possible, including the recording of all milestones and target dates for completion.

6.3.2 Updating a POA&M

The ISSO is responsible for submitting updates on each POA&M on at least a quarterly basis until resolution. These updates are maintained for each milestone using the CFACTS tool. HVA system POA&Ms must have monthly updates including vulnerability scan reports to HHS. The following steps detail the process for submitting monthly updates for the POA&M milestones:

- **Step 1:** The ISSO or support contractor locates the POA&M in CFACTS using the subtasks below:
  - Login to CFACTS and select the "*Assessment & Authorization (A&A)*" tab from the top menu.
  - Click on "Authorization Package – Records" under the "Quick Links" column and select the appropriate information system from the list. You may also find the information system by clicking "Search Records" and specifying search criteria.
  - Once the information system has been located click on the system name to open the authorization package for the system.
  - Select the *"Controls"* tab from the top navigation tab of the authorization package.
  - Scroll down to the *"Allocated Controls"* section to locate the hyperlinks for the POA&Ms associated with the controls with a status of "Other Than Satisfied".

- Click the hyperlink for a POA&M to open that POA&M. Scroll down to the *"Milestone"* section, locate the milestone and click *"View"* to the left of the milestone.

- **Step 2:** Click the *"Edit"* button to switch to edit mode. Scroll down to the *"Milestone Changes"* section and add comment indicating the updated status for the milestone. Include the date of comments (e.g. xx/xx/xxxx). Append to the comments each month so that a complete history of the status of that milestone is maintained.
  - ***NOTE: If a milestone is delayed, and the delay will result in the POA&M closure exceeding the schedule completion date then an "Estimated Completion Date"* should be entered in the *"milestone changes"* section. Provide a justification in the *"Milestone Changes"* box indicating the reason for the delay.**
- **Step 3:** Click *"Save"* in the upper left hand corner of the *"Milestones"* window to save the updates to the milestone.

6.3.3 Closing a POA&M

To close a POA&M, a remediation package containing artifacts demonstrating that the weakness has been mitigated must be submitted and approved by the ISSO using the CFACTS tool. The CRA verifies mitigation for all high risk weaknesses and a sample of moderate and low risk weaknesses. The following steps detail the process for uploading evidence and closing a POA&M:

- **Step 1:** The ISSO or support contractor locates the POA&M in CFACTS using the subtasks below:
  - Login to CFACTS and select the "Assessment & Authorization (A&A)" tab from the top menu
  - Click on "Authorization Package – Records" under the "Quick Links" column and select the appropriate information system from the list. You may also find the information system by clicking "Search Records" and specifying search criteria
  - Once the information system has been located click on the system name to open the authorization package for the system
  - Select the "Controls" tab from the top navigation tab of the authorization package
  - Scroll down to the "Allocated Controls" section to locate the hyperlinks for the POA&Ms associated with the controls with a status of "Other Than Satisfied"
  - Click the hyperlink for a POA&M to open that POA&M
- **Step 2:** Scroll down the *"Remediation Evidence"* section and click *"Add New"* in the top right hand corner.
- **Step 3:** Click the *"Select Files"* button browse the files containing the remediation evidence and double click them to add them to the *"files to upload"* box. Click *"Ok"* to upload the files.
- **Step 4:** Scroll down to the *"POA&M Submission"* section select a POA&M Owner, change the POA&M status to *"Submit for Review"* and select a submit date.
- **Step 5:** The ISSO reviews the evidence package and documents that review in the *"Review"* section of the associated POA&M in CFACTS. If the ISSO concurs with the evidence package, the status of the POA&M is updated to *"Completed"* and the POA&M

is now closed. If the ISSO does not concur with the evidence package, then they work with the necessary stakeholders to obtain new evidence to support the closure of the POA&M. A "*Completed"* weakness shall remain on the POA&M report for one year after it is closed.

6.3.4 Risk Acceptance

If the weakness that prompted the creation of a POA&M cannot be mitigated then the risk may be accepted. Risk acceptance is a common and appropriate practice within an organization. When the risk response with the identified risk is within the organization's risk tolerance and/or the risk has been sufficiently mitigated to an acceptable level, the organization may choose to accept the risk. The accepted risk shall be documented in the system's ISRA and should include justification as to why the risk cannot be mitigated. Risk deemed to be low, moderate, or high can be accepted depending on particular situations or conditions which are unique to the organization. For example, organizations with data centers residing in the northeastern portion of the United States may opt to accept the risk of earthquakes based on known likelihood of earthquakes and data center vulnerability to damage by earthquakes. Organizations accept the fact that earthquakes are possible, but given the infrequency of major earthquakes in that region of the country, believe it is not cost-effective to address such risk—that is, the organizations have determined that risk associated with earthquakes is low, due to the likelihood of a non-occurrence, and therefore acceptable. Conversely, organizations may accept substantially greater risk (in the moderate/high range) due to compelling mission, business, or operational needs. Organizations typically make determinations regarding the general level of acceptable risk and the types of acceptable risk with consideration of organizational priorities and trade-offs between: (i) near-term mission/business needs and potential for longer-term mission/business impacts; and (ii) organizational interests and the potential impacts on assets such as individuals and information systems.[5] Some scenarios requiring a Risk Acceptance are:

- When the cost of implementing the control is more than the benefit gained
- When implementation of the control results in adverse effects to functionality of the system
- It is technically infeasible to implement the control
- When implementing the control results in disrupting the business process

This list is by no means exhausting and provides some of the most common scenarios for Risk Acceptance.

6.4 Security Authorization (CA-6)

Security authorizations are official management decisions that are conveyed through authorization decision documents by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. The CIO serves as the authorizing official for CMS. The CIO is responsible

[5] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

for making an overall determination of risk and authorizing CMS information systems for operation, if it is determined that the associated risk are acceptable. An Authorization to Operate (ATO) memo is signed by the CIO giving the System Owner/BO formal authority to operate a CMS information system.

The CMS Cybersecurity Integration Center (CCIC) must be notified when significant changes occur to architecture, security posture, or other items that could cause degradation or unexpected results in security monitoring, detection, response, and mitigation activities prior to making the changes. Some examples of significant changes that may occur are:

- Discovery of a new vulnerability
- New COTS tool integration
- Installation of a new operating system
- Modifications to system ports, protocols, or services
- Installation of new hardware platform
- Modifications to security controls

Notification of significant changes will be sent via email by the System Owner/BO to the CCIC.

The table below outlines the ODPs for security authorization:

Table 7: CMS Defined Parameters – Control CA-6

Control	Control Requirement	CMS Parameter
CA-6	The organization: c. Updates the security authorization [Assignment: organization-defined frequency].	c. Updates the security authorization: • Within every three (3) years; • When significant changes are made to the system; • When changes in requirements result in the need to process data of a higher sensitivity; • When changes occur to authorizing legislation or federal requirements that impact the system; • After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and • Prior to expiration of a previous security authorization.

NIST requires three artifacts to support the authorization decision for information systems: System Security Plan (SSP), Security Assessment Report (SAR), and Plan of Actions and Milestones

(POA&M). At CMS, additional documentation is included and considered as a basis for making an ATO recommendation to the CIO. The following list contains the CMS specific artifacts required for a complete authorization package:

- SSP
- SAR
- POA&M
- Contingency Plan (CP)
- CP Test Plan
- CP Test After Action Report
- Information System Risk Assessment (ISRA)
- Privacy Impact Assessment (PIA)
- Interconnection Security Agreement (ISA) – *if applicable*

The following steps detail the CMS specific process for requesting and receiving an ATO for a CMS information system.

- **Step 1:** The ISSO completes the CMS System Authorization ATO Request form (see Appendix G) and uploads the completed form to the CFACTS tool using the subtasks below:
    - Login to CFACTS and select the *"Assessment & Authorization (A&A)"* tab from the top menu
    - Click on "Authorization Package – Records" under the "Quick Links" column and select the appropriate information system from the list. You may also find the information system by clicking "Search Records" and specifying search criteria
    - Once the information system has been located, click on the system name to open the authorization package for the system.
    - Select the *"Authorization"* tab from the top navigation tab of the authorization package.
    - Click the *"Edit"* button at the top of the authorization package window.
    - Click *"Add New"* and then click *"Select File(s)"* to navigate the completed CMS System Authorization ATO Request Form. Save form. Add Authorization ATO Request Form section of the Authorization tab. After attaching the form, click "OK" to return the authorization package window.
    - Sends an email to their CRA, cc CISO MB notifying them that the CMS System Authorization ATO Request Form uploaded to CFACTS and that the authorization package is ready for review.
    - Set Authorization Package Submission Status to "Submitted".
- **Step 2:** The CRA requests an ATO package review by their support staff.
- **Step 3:** The CRA support staff conducts a review of the ATO package by completing the ATO Gating Review Checklist. If updates to the ATO package are required, the support staff notifies the CRA whom then works with the ISSO to make the necessary updates.
- **Step 4:** Once the CRA is satisfied that the authorization package meets the CMS criteria, the CRA sends a request to their supporting contractor to draft the ATO memo and executive summary.

- **Step 5:** The CRA receives the draft ATO memo and executive summary from the support contractor, updates the executive summary as necessary, and creates a red folder with the following ATO documentation:
    - POA&M Report
    - Executive Summary
    - ATO Memo
- **Step 6:** The CRA submits the red folder to the assigned privacy lead for review and comment. If updates are identified by the privacy lead, the CRA works with the ISSO to make those changes and updates the red folder package as necessary.
- **Step 7:** The CRA submits the red folder package to the Director of the Division of Security, Privacy Policy and Governance (DSPPG) and the Director of the Division of Security and Privacy Compliance (DSPC) for sign-off working with the ISSO to update the package as needed based on the feedback from the directors.
- **Step 8:** The DSPC Director takes the red folder package to the CISO for review and approval. If updates are identified by the CISO, the CRA works with the ISSO to make those changes and updates the red folder package as necessary.
- **Step 9:** The CISO presents the ATO memo to the CIO for signature and briefs the CIO on the risks associated with the information system and any associated POA&Ms identified to mitigate those risks.
- **Step 10:** The CIO signs the ATO memo. The CIO returns the signed ATO memo to the CRA.
- **Step 11:** The CRA uploads the signed ATO memo into the CFACTS tool and updates the ATO expiration date, and Date Authorization Memo signed in the system to reflect the newly issued ATO.

6.5 Continuous Monitoring (CA-7)

Information Security Continuous Monitoring (ISCM) programs raise awareness regarding threats, vulnerabilities, and information security in support of organizational risk management decisions. Continuous implies that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. An ISCM program is designed to collect information according to established metrics, utilizing information readily available in part through existing security controls. This program integrates with the Assess, Authorize, and Monitor phases of the Risk Management Framework and enables Ongoing Authorization (OA) of information systems.

CMS, along with other federal agencies, plans to transition from point-in-time authorizations to the more dynamic OA. This process is still based on an initial system authorization (**See CA-6**) and must have a valid ATO, but systems that enter OA have ATO letters that do not expire. Ongoing Authorization is enabled by having ISCM capabilities in place, but the continuous monitoring capabilities must be mature enough before the transition to ongoing authorizations can occur.

As part of the US Government's efforts to enhance security of federal information systems, agencies across the government are required to establish an ISCM program.[6] DHS provides the primary guidance for HHS and for the CMS Continuous Monitoring program.

CMS has implemented a continuous monitoring program at the CMS Cybersecurity Integration Center (CCIC). The CCIC ensures oversight of information security and privacy, including Security Information Event Management (SIEM), for each FISMA System operating by or on behalf of CMS. The CCIC delivers various agency-wide security services[7]. These services include Continuous Diagnostics and Mitigation (CDM) as well as security engineering, incident management, forensics and malware analysis, information sharing, cyber threat intelligence, penetration testing, and software assurance. In order for CMS to monitor security information across the enterprise, there must be connectivity between the data sources and CMS to allow for effective continuous monitoring. In addition, the Continuous Monitoring strategy ties in with other stakeholder plans and strategies, including Incident Response[8].

[6] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

[7] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-II-%E2%80%93-Network-Services.html?DLPage=1&DLEntries=10&DLFilter=tra&DLSort=0&DLSortDir=ascending

[8] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf

Figure 2: How CDM Works[9]

The table below outlines the CMS organizationally defined parameters for continuous monitoring:

Table 8: CMS Defined Parameters – Control CA-7

Control	Control Requirement	CMS Parameter
CA-7	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of defined metrics (defined by the CCIC CDM Program[10]) to be monitored based on the organization security goals and objectives and in accordance with the basic requirements set forth in NIST SP 800-137; b. Establishment of defined frequencies (defined by the CCIC CDM Program) for monitoring and defined frequencies (defined by CCIC CDM Program) for assessments supporting such monitoring;

The Continuous Monitoring strategy guides the implementation through phases of an Information Security Continuous Monitoring (ISCM) program. The CCIC is responsible for the initial focus on Phase 1, which incorporates endpoint protection by conducting an inventory of what is on the network through Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VUL).

[9] https://www.dhs.gov/cdm

[10] For a copy of the requirements, please send an email to CMS CCIC

Figure 3: CDM Program Phases[11]

The requirements for the four phases of the CDM program are directed from DHS; the CCIC will ensure that automated and manual monitoring efforts are in place. Guidance from the CCIC will continue with each update to the program and increased implementation of the phases.

6.5.1 Continuous Monitoring | Independent Assessment (CA-7(1))

CMS conducts Security Control Assessments (SCA) in support of its Continuous Monitoring strategy. To ensure that an impartial assessment is performed on system controls, the CCIC provides independent assessments on thirty (30) published controls. These assessments must be conducted no less frequent than one-third every year ensuring that all systems are assessed during the 3-year cycle.

Table 9: CMS Defined Parameters – Control CA-7(1)

Control	Control Requirement	CMS Parameter
CA-7(1)	The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security	The organization employs the CCIC to monitor the security controls in the information system on an ongoing basis.

[11] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2016-10/cdm_program-overview.pdf

	controls in the information system on an ongoing basis.	

6.6 Penetration Testing (CA-8)

Penetration testing is performed on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing is used to validate vulnerabilities or determine the degree of resistance that organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). This type of testing attempts to duplicate the actions of internal and external adversaries in carrying out hostile cyber-attacks against the organization and allows a more in-depth analysis. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls.

CMS has the ability to choose internal or external penetration testing teams; penetration testing is one of the services provided by the CCIC. For each penetration test, there must be an agreed upon Rules of Engagement (RoE) before the test can occur. The RoE ensures that a penetration test will be effective and safe for the environment and for those involved in the test itself. CMS utilizes its own RoE for penetration tests that can be found in Appendix I of this document.

Penetration testing is performed on all High Value Assets (HVA) information systems within CMS at a frequency of every three hundred sixty-five (365) days or when there has been a significant change to the system. Information covering significant changes and the systems that will be tested must be updated in the SSP.

Table 10: CMS Defined Parameters – Control CA-8

Control	Control Requirement	CMS Parameter
CA-8	The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].controls in the information system on an ongoing basis.	The organization conducts both internal and external penetration testing, within every three hundred sixty-five (365) days, on defined information systems or system components (defined in the applicable system security plan), or whenever there has been a significant change to the system. As a minimum, penetration testing must be conducted to determine: a. How well the system tolerates real world-style attack patterns; b. The likely level of sophistication an attacker needs to successfully compromise the system; c. Additional countermeasures that could mitigate threats against the system; and d. Defenders' ability to detect attacks and respond appropriately. Penetration testing is required under OMB M-17-09 for all systems defined as High Value Assets (HVAs)

Below are the procedural steps to facilitate a penetration test in the CMS environment:

- **Step 1:** Through oversight responsibilities, CRAs and / or ISSOs can request a penetration test to be performed by the CCIC. This test can provide some technical results and assurances on the security of the system. CRAs can work with system ISSOs to determine if this option is beneficial and informative on a system's risk posture.
- **Step 2:** After the decision is made to conduct the test, the CRA should contact the ISSO of the system to be tested and obtain the IP address and/or Uniform Resource Locator (URL) for the system.
- **Step 3:** The CRA oversees the sending of the IP address and/or URL to the Division of Cyber Threat and Security Operations (DCTSO) Penetration Testing Lead.
- **Step 4:** DCTSO staff will set-up a kick-off meeting with the stakeholders, ISSO, CRA, BO, and any Contractors, involved with the system(s) to determine the scope of the penetration test.
    - ISSOs and BOs will ensure that the meeting invite is forwarded to any other personnel, based on the involvement with the application.
    - During the meeting, the penetration test team will relay what type of accounts are needed to perform the test, i.e. user and/or admin accounts, etc.
- **Step 5:** After determining the scope of the penetration test, DCTSO will add the application to the penetration test schedule and inform the CRA, ISSO, and BO of the date that the penetration testing will begin and its projected duration.
- **Step 6:** Upon completion of penetration test, an out-brief between the BO and Penetration Testing team is performed to discuss test results and the discovery of all findings.
- **Step 7:** The system's BO has one (1) week to mitigate findings, focusing first on the highest risk findings.
- **Step 8:** Penetration testers will confirm that the findings are remediated by retesting closed findings within the remediation timeframe.
- **Step 9:** The final report can be obtained from The Incident Management Team (IMT). The email address for IMT is IMT@CMS.HHS.GOV
- **Step 10:** The CRA will work with the ISSO to create the CAAT worksheet, ensuring accuracy and completeness, for any remaining findings after the remediation week concludes.
- **Step 11:** The CRA, as oversight, ensures that each CAAT worksheet is accurately uploaded into CFACTS within thirty (30) days from the date the finding was discovered.

- **Step 12:** Any deviations to this process should be reviewed and evaluated for their risk to the security posture of systems.

6.7 Internal System Connections (CA-9)

This control applies to connections between organizational information systems and separate constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

For CMS, there is a requirement to include privacy standards in connection documents. For example, an Interconnection Security Agreement (ISA) is required for external system connections. In addition, documentation shall be created addressing responsibilities of the receiving information system for how it will protect the Personally Identifiable Information (PII) which transits the system.

The table below outlines the CMS organizationally defined parameters (ODPs) for internal system connections:

Table 11: CMS Defined Parameters - Control CA-9

Control	Control Requirement	CMS Parameter
CA-9	The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system	The organization: a. Authorizes connections of defined internal information system components or classes of components (defined in the applicable system security plan) to the information system;

- **Step 1:** The System Owner shall define information system components or classes of components (found in the applicable SSP) to be authorized as internal connections to the information system.
- **Step 2:** The System Owner shall authorize internal connections of organization-defined information system components or classes of components to the information system when the ATO memo is signed.
- **Step 3:** The System Owner shall document the (1) interface characteristics; (2) the security requirements; and (3) the nature of the information communicated for each internal connection within the applicable SSP.

Appendix A. Acronyms

Selected acronyms used in this document are defined below.

Acronyms	Terms
AO	Authorization Official
ARS	Acceptable Risk Safeguards
CCIC	CMS Cybersecurity Integration Center
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
CMS CO	CMS Contracting Officers
CMS IS	CMS Information Security
CMS IS2P2	CMS Information Systems Security and Privacy Policy
CRA	Cyber Risk Advisor
FISMA 2014	Federal Information Security Modernization Act of 2014
FTI	Federal Tax Information
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IMT	Incident Management Team
IR	Incident Response
IRA	Incident Response Authority
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IRT	Incident Response Team
ISO	Information Systems Owners

Acronyms	Terms
ISPG	Information Security and Privacy Group
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
ODP	Organizational Defined Parameters
OPDIV	Operating Divisions
OS	Operating System
PHI	Protected Health Information
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
POA&Ms	Plan of Action and Milestones
POC	Point of Contact
Pre-BAT	Pre-Breach Analysis Team
RMH	Risk Management Handbook
SCA	Security Controls Assessment
SCAP	Security Content Automation Protocol
SIEMs	Security Information Event Management
SOC	Security Operations Center
SOP	Senior Official for Privacy
SP	Special Publication
SSP	System Security Plan
URL	Universal Resource Locator
US-CERT	United States Computer Emergency Readiness Team

Appendix B. Glossary of Terms

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

Terms	Definitions
Acceptable Risk Safeguards	CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR),” http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity.
After Action Report	A document containing findings and recommendations from an exercise or a test.
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.
Breach	A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Breach Analysis Team	An information security and privacy incident and breach response team with the capability that includes preparation, identification, containment, eradication, recovery, and follow-up capabilities to ensure effective recovery from information security and privacy incidents and breaches.
Centers for Medicare & Medicaid Services	CMS covers 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace.
Chief Information Officer	1. 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

Terms	Definitions
Chief Information Security Officer	The incumbent in the position entitled Chief Information Security Officer. The CISO must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 11, OpDiv CISOs. The CISO carries out the CIO's information security responsibilities under federal requirements in conjunction with the SOP.
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 database that maintains current FISMA information (e.g., POCs, artifacts) to support organizational requirements and processes (e.g., communication, contingency planning, training, data calls).
CMS Minimum Security Requirements	Description of the minimum requirements necessary for an information system to maintain an acceptable level of security.
CMS IT Service Desk	For the purposes of incident response coordination, the CMS IT Service Desk is a sub-component of the CMS Information Security and Privacy Group and IMT, whose responsibilities include but are not limited to the following: • Act as the first point of contact for security incidents or anomalies, and record information provided by the system user, CMS Business Owner/Information Systems Owner (ISOs) or On-site Incident Response Authority (IRA) , depending on alert source • Generate a CMS incident ticket to document the incident for CMS records • Determine if the incident relates to PII • Immediately refer information security incidents to the IMT
Cyber Risk Advisor	Act 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).

Terms	Definitions
Event	An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.
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 Tax Information (FTI)	Federal Tax Returns and return information are confidential, as required by Internal Revenue Code (IRC) Section 6103. The information is used by the Internal Revenue Service (IRS) is considered FTI and ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality. [IRS 1075] Tax return information that is not provided by the IRS falls under PII.
Health Insurance Portability and Accountability Act of 1996	An act that amended 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 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 IRT reports to the CMS CCIC IMT, which is responsible for CMS-wide incident management.

Terms	Definitions
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
Incident Management Team	CMS IMT provides 24X7 incident management support for the enterprise. It is a single communication point for CMS leadership for security incidents and updates.
Incident Response	Incident response outlines steps for reporting incidents and lists actions to resolve information systems security and privacy related incidents. Handling an incident entails forming a team with the necessary technical capabilities to resolve an incident, engaging the appropriate personnel to aid in the resolution and reporting of such incidents to the proper authorities as required, and report closeout after an incident has been resolved.
Individual Health Information	Individually Identifiable Health Information is a subset of health information including demographic data collected concerning an individual that: • Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse • Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual or the past, present, or future payment for the provision of healthcare to an individual, and meets either of the following: • Identifies the individual • There is a reasonable basis to believe the information can be used to identify the individual
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 subject to federal law, regulation, and guidance.
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,

Terms	Definitions
	evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by the executive agency directly or is used by a contractor, under a contract with the executive agency; or use 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). This includes 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. In 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.
Insider Threat	An insider threat generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network (system or data). Intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.1 Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware as Insiders, facilitate aiding a threat actor (i.e., the unintentional insider threat). It is vital that organizations understand normal employee baseline behaviors and ensure employees understand how being used as conduit information can be obtained.
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

Terms	Definitions
	Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974 ("Privacy Act"). The Privacy Act addresses CMS applicable information security and privacy requirements, arising from federal legislation, mandates, directives, executive orders. The 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.
Privacy Incident	A Privacy Incident is a Security Incident that involves Personally Identifiable Information (PII) or Protected Health Information (PHI), or Federal Tax Information (FTI) where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users or any other than authorized purposes. Users must have access or potential access to PII, PHI, and/or FTI in usable form whether physical or electronic. Privacy incident scenarios include, but are not limited to: • Loss of federal, contractor, or personal electronic devices that store PII, PHI and/or FTI affiliated with CMS activities (i.e., laptops, cell phones that can store data, disks, thumb-drives, flash drives, compact disks, etc.) • Loss of hard copy documents containing PII, PHI and/or FTI • Sharing paper or electronic documents containing PII, PHI and/or FTI with individuals who are not authorized to access it • Accessing paper or electronic documents containing PII, PHI and/or FTI without authorization or for reasons not related to job performance • Emailing or faxing documents containing PII, PHI and/or FTI to inappropriate recipients, whether intentionally or unintentionally • Posting PII, PHI and/or FTI, whether intentionally or unintentionally, to a public website • Mailing hard copy documents containing PII, PHI and/or FTI to the incorrect address • Leaving documents containing PII, PHI and/or FTI exposed in an area where individuals without approved access could read, copy, or move for future use
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.

Terms	Definitions
	Note: PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer.
Personal Identifiable Information	Any information about an individual including, but not limited to: education, financial transactions, medical history, and criminal or employment history; and information which can be used to distinguish or trace an individual's identity, such as the name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual. Information which can be used to distinguish or trace an individual's identity, such as the name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Risk	The likelihood that a threat will exploit a vulnerability. For system may not have a backup power source; hence, it is vulnerable to a threat, such as thunderstorm, which creates a risk.
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.
Scenario	A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.
Security Incident	In accordance with *NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide*, a security incident is defined as an event that meets one or more of the following criteria: • The successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system processing information on behalf of CMS. It also means the loss of data through theft or device misplacement, loss or misplacement of

Terms	Definitions
	hardcopy documents and misrouting of mail, all of which may have the potential to put CMS data at risk of unauthorized access, use, disclosure, modification, or destruction • An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits • A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
Security Support Structure Configuration Modification	A type of malicious software (Malware) - Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled. SSS is essential to maintaining the security policies of the system, unauthorized modifications to these configurations can increase the risk to the system.
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, OpDiv SOP. The SOP carries out the CIO's privacy responsibilities under federal requirements in conjunction with the CISO.
Spyware	A type of malicious software (Malware) that has surreptitiously installed and intended to track and report the usage of a target system, or collect other data the author wishes to obtain.
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environmental specified in an IT plan.
Test Plan	A document that outlines the specific steps performed for a particular test, including the required logistical items and expected outcome or response for each step.
Threat(s)	The potential to cause unauthorized disclosure, changes, or destruction to an asset. • **Impact:** potential breach in confidentiality, integrity, failure and unavailability of information • **Types:** natural, environmental, and man-made
Training	Informing personnel of roles and responsibilities within a particular IT plan and teaching personnel skills related to those roles and responsibilities.
Vulnerabilities	Any flaw or weakness that can be exploited and may result in a breach or a violation of a system's security policy.

Appendix C. Applicable Laws and Guidance

Appendix C provides references to both authoritative and guidance documentation supporting the "document." Subsections are organize to "level of authority" (e.g., Statues take precedence over Federal Directives and Policies). The number on each reference represents a mapping that uniquely identifies the reference within the main body of the document. The brackets [#] in the Roles and Responsibilities section are the actual brackets in the "Policy." In this document, the brackets serve as an example of how the brackets will appear in both sections of the document.

C.1 Statutes

1 Federal Information Security Modernization Act (FISMA) of 2014
https://www.congress.gov/bill/113th-congress/senate-bill/2521

2 Health Insurance Portability and Accountability Act of 1996 (HIPAA)
http://www.hhs.gov/hipaa/

3 The Privacy Act of 1974, as amended (5 U.S.C. 552a)
http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/PrivacyActof1974.html

C.2 Federal Directives and Policies

1 Code: 5 U.S.C. §552a(e)(10)

http://www.gpo.gov/fdsys/granule/USCODE-2010-title5/USCODE-2010-title5-partI-chap5-subchapII-sec552a/content-detail.html

2 E-Government Act of 2002 (Pub. L. No. 107-347) § 208

https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html

3 FedRAMP Rev. 4 Baseline

https://www.fedramp.gov/files/2015/03/FedRAMP-Control-Quick-Guide-Rev4-FINAL-01052015.pdf

C.3 OMB Policy and Memoranda

1 OMB Circular A-130 Management of Federal Information Resources

http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

2 OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*

http://www.whitehouse.gov/omb/memoranda_m03-22/

3 OMB M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

4 OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

C.4 NIST Guidance and Federal Information Processing Standards

1 FIPS-199 *Standards for Security Categorization of Federal Information and Information Systems*

http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

2 NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*.

http://dx.doi.org/10.6028/NIST.SP.800-18r1

3 NIST SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems*

http://dx.doi.org/10.6028/NIST.SP.800-37r1

4 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

5 NIST SP 800 53Ar4 *Guide for Assessing the Security Controls in Federal Information Systems*

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

6 NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*

http://dx.doi.org/10.6028/NIST.SP.800-83

7 US-CERT Federal Incident Notification Guidelines

https://www.us-cert.gov/incident-notification-guidelines

8 NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*

http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

9 NIST Special Publication 800-137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.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. To obtain 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 Office of Grants and Acquisition Policy and Accountability (OGAPA)*

http://www.hhs.gov/about/agencies/asfr/ogapa/

5 *HHS-OCIO-2008-0001.003 HHS Policy for Responding to Breaches of Personally Identifiable Information*

http://www.hhs.gov/ocio/policy/20080001.003.html

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/Downloads/IS2P2.pdf

2 *CMS Office of Acquisition and Grants Management (OAGM)*

https://www.cms.gov/About-CMS/Leadership/oagm

3 *Risk Management Manual 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

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 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

3 CMS Technical Reference Architecture Volume I - Foundation Version 1.0 June 28, 2016

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-I-%E2%80%93-Foundation.html

4 CMS Technical Reference Architecture Volume IV – Development and Application Services

Version 1.0 June 28, 2016

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

5 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

6 Risk Management Handbook Chapter 14 Risk Assessment

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix D. Security Assessment Plan Template

The RMH Chapter 4 Security Assessment and Authorization Appendix D – Security Assessment Plan Template is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix E. Security Assessment Report Template

The RMH Chapter 4 Security Assessment and Authorization Appendix E – Security Assessment Report Template is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix F. CAAT Spreadsheet Template

The RMH Chapter 4 Security Assessment and Authorization Appendix F – CAAT Spreadsheet Template is available on the CFACTS website home page located at:

https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx#home

Appendix G. CMS System ATO Request Form

The RMH Chapter 4 Security Assessment and Authorization Appendix G – CMS System ATO Request Form is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix H. Interconnection Security Agreement Template

The RMH Chapter 4 Security Assessment and Authorization Appendix H – Interconnection Security Agreement Template is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix I. Rules of Engagement Template

The RMH Chapter 4 Security Assessment and Authorization Appendix I – Rules of Engagement Template is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix J. Data Agreement Guidance

The RMH Chapter 4 Security Assessment and Authorization Appendix J – Data Agreement Guidance is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix K. Memorandum of Understanding (MOU)

The RMH Chapter 4 Security Assessment and Authorization Appendix L – Memorandum of Understanding is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix L. Feedback and Questions

Information security and privacy are dynamic fields 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 ISPG Policy mailbox at ISPG_Policy_Mailbox@cms.hhs.gov. Your feedback will be evaluated for incorporation into future releases of the document. Questions about any of the material include within this document may also be sent to the ISPG Policy mailbox.