Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Risk Management Handbook (RMH) Chapter 2: Awareness and Training

Final

Version 1.0

February 15, 2019

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
1.0	2/15/2019	All	ISPG	Final Publication

Effective Date/Approval

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effective on the date that CMS' Deputy Chief Information Security Officer signs it and remains in effect until it is rescinded, modified or superseded.

Signature: Kevin A. Dorsey -S

Digitally signed by Kevin A. Dorsey -S
Date: 2019.02.27 11:34:50 -05'00'

Date of Issuance: February 21, 2019

Kevin Allen Dorsey
CMS Deputy Chief Information Security Officer (DCISO)

Table of Contents

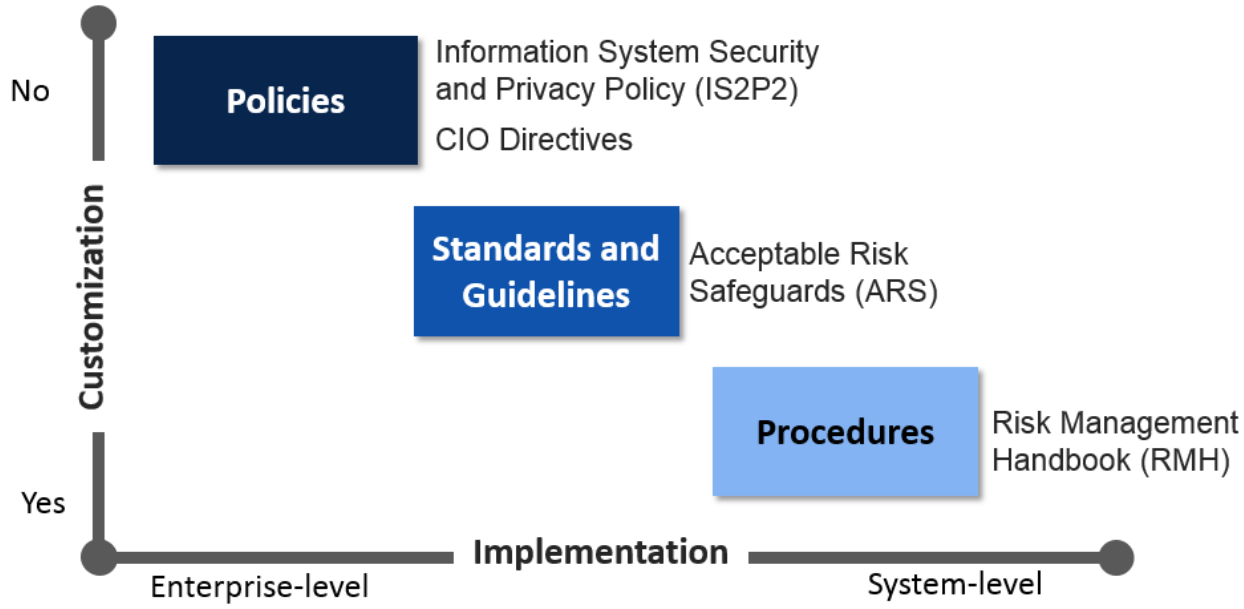
Tables

Figures

1. Introduction

1.1 Purpose

The Centers for Medicare & Medicaid Services (CMS) Risk Management Handbook (RMH) Chapter 2 Awareness and Training 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:



This document describes procedures that facilitate the implementation of security controls associated with the Awareness and Training (AT) family of controls. To promote consistency among all RMH Chapters, CMS intends for Chapter 2 to align with guidance from the National Institute of Standards and Technology (NIST), 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 Awareness and Training 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 2 provides processes and procedures to assist with the consistent implementation of the AT 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 AT 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 AT control family that an organization must define, develop, disseminate, review, and update its documentation at least once every three years. 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 policy and associated controls.

The Risk Assessment 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
- 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

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

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 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 requirements prescribed in standards with the objective of enabling consistency across the CMS environment. The CMS environment includes users, networks, devices, all software, processes, 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.

[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

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 Awareness and Training (AT) Control	HIPAA Section
Security Awareness Training (AT-2)	§164.308(a)(5)
Role-Based Security Training (AT-3)	§164.308(a)(2); §164.308(a)(3)(i); §164.308(a)(5)(i); §164.308(a)(5)(ii)(A); §164.308(a)(5)(ii)(B); §164.308(a)(5)(ii)(C); §164.308(a)(5)(ii)(D)

[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

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.

Role	Applicable Controls
All Users	AT-2; AT-2(2); AT-3, AT-4
CMS Business Owner (BO)	AT-4
CMS Contracting Officer (CO) and Contracting Officer's Representative (COR)	AT-4
CMS Chief Information Security Officer	AT-4

6. Procedures

Procedures assist in the implementation of the required security and privacy controls. In this section, the AT family procedures are outlined. To increase traceability, each procedure maps to the associated NIST controls using the control number from the CMS IS2P2.

6.1 Security Awareness Training (AT-2)

The purpose of Security and Privacy Awareness Training prepares users to manage security and privacy risks through a broad campaign that introduces them to the concepts, scenarios, and tools used to compromise information security and privacy protections. The content for security awareness training differs from organization to organization and is dependent on specific organizational requirements including personnel that have permissions to different types of data. Common security awareness techniques include but are not limited to displaying informational posters, emails, office supplies with security reminders printed on them, security messages during logons, and conducting information security awareness events.

The table below outlines the CMS organizationally defined parameters (ODPs) for AT-2.

Table 1: CMS Defined Parameters – Control AT-2

Control	Control Requirement	CMS Parameter
AT-2	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): c. [Assignment: organization-defined frequency] thereafter.	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): c. Within every three hundred sixty-five (365) days thereafter.

CMS provides information security awareness training to all users with Enterprise User Administration (EUA) accounts, including managers, senior executives, and contractors, which is delivered through the Computer Based Training (CBT) system. Users without EUA access should contact their Contracting Officer (CO) or Contracting Officer Representative (COR) for direction. The following steps detail CMS' process for security awareness training:

Initial Certification:

- **Step 1:** On the Employee Onsite Date (EOD), the User receives a CMS user ID activation Welcome email from Enterprise User Administration (EUA). Users are given seven (7) calendar days to complete CBT.
    - EUA sends reminder emails on a daily basis until certification is complete.
- **Step 2:** The User logs in and completes the CBT.
- **Step 3:** Once CBT is completed, the EUA system tracks the completed training. An option to print the completion certificate is available, but it is not required.

Recertification:

- **Step 1:** Recertification is to be completed annually on the User ID activation month. The EUA system sends an email notification to the user at forty-five (45) days in advance of the recertification due date.
    - Email reminders to complete recertification are sent at 15, 10, 5, 4, 3, 2, and 1 day(s) until revocation date.
- **Step 3:** The User logs in to the EUA system and completes the CBT.
- **Step 4:** If the User does not complete the training within the recertification timeframe, revocation occurs on the first day of the month following their due date. In the event of a revocation, contact the CMS IT Service desk at 410-786-2580 or cms_it_service_desk@cms.hhs.gov.

6.1.1 Security Awareness Insider Threat (AT-2(2))

The purpose of Security Awareness Insider Threat is to ensure that security awareness training reinforces the identification and reporting of potential indicators of insider threat. Security awareness training includes how to communicate concerns from employees and management regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

Included in the security awareness and training (see AT-2 above) is identifying and reporting potential indicators of insider threats, such as:

a. Inordinate, long-term job dissatisfaction,
b. Attempts to gain access to information not required for job performance,
c. Unexplained access to financial resources,
d. Bullying or sexual harassment of fellow employees,
e. Workplace violence, and
f. Other serious violations of organizational policies, procedures, directives, rules, or practices.

6.2 Role-Based Security Training (AT-3)

The purpose of Role-Based Training (RBT) is to determine and complete the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals, the specific security requirements of the organization, and the information systems to which personnel have authorized access. A comprehensive role-based training program addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures.

CMS defines a role with significant information security and privacy responsibilities as any role that has the potential to adversely impact the security posture of one or more CMS systems when the system is operational. CMS provides the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of CMS' information security and privacy programs. Training on policies, procedures, tools, and artifacts for the organizational security and defined privacy roles are some examples provided in the training program. Role-based security and privacy training requirements also applies to contractors providing services to CMS.

The table below outlines the CMS organizationally defined parameters (ODPs) for AT-3.

Table 2: CMS Defined Parameters – Control AT-3

Control	Control Requirement	CMS Parameter
AT-3	The organization provides role-based security training to personnel with assigned security roles and responsibilities:	The organization provides role-based security training to personnel (both contractor and employee) with assigned information security and privacy roles and responsibilities (i.e., significant information security and privacy responsibilities):
	c. [Assignment: organization-defined frequency] thereafter.	c. Within sixty (60) days of entering a position that requires role-specific training, and within every 365 days thereafter.

The instructions for the identification of federal employees with significant information security and privacy responsibilities (SSR) and RBT requirements are detailed in data calls conducted by Office of Human Capital (OHC). CMS managers must participate in any such data calls.

The instructions for the identification of Contractors with SSR and RBT requirements are detailed in the following steps:

- **Step 1**: Review the definition of SSR as provided in the CMS IS2P2.
- **Step 2**: Identify all positions that include duties involving SSR. Each of these positions with SSR requires (RBT).

- **Step 3:** For each job position, determine appropriate RBT by reviewing NIST SP 800-181[5], the NICE Cybersecurity Workforce Framework. Select the NICE role(s) that aligns with each job position. Each position may receive no more than three (3) NICE roles and should be documented in the order in which the most critical function of the job is listed first; the next critical function of the job is listed next, and so on.
- **Step 4:** All personnel in a position with SSR are to be notified. This notice should include the NICE role assignments for the job position.
- **Step 5:** This process should be followed when new job positions are created, and when there are changes to an existing position that involve significant information privacy and security responsibilities.

RBT courses must focus on the knowledge, skills, and abilities to fulfill the IT and cybersecurity responsibilities for the specific role category. While Contractors are required to receive and track their own role-based security training, CMS must ensure RBT is available for personnel (both contractor and employee) with significant information security and privacy responsibilities. CMS encourages personnel to leverage the training sessions that are offered in the form of briefings, forums, seminars, professional development workshops, conferences, and professional independent reading and research. Such training focuses on improving the information security and privacy skills and competencies of personnel managing, designing, developing, acquiring, and administering CMS' resources. Employees and Contractors can select CMS offered training by accessing the ISPG provided Cybersecurity and Privacy Training Catalog in Appendix E.

Employees and Contractors may additionally select other qualified training offerings available from government or industry. As training offerings are increasingly mapped to the NIST NICE Framework, employees and contractors can identify training aligned with NICE role assignments.

For training offerings that have not been mapped to the NIST NICE Framework, the following provides evaluation steps:

- **Step 1:** Know the NICE role-based training ID that is to be trained.
- **Step 2:** Refer to the NIST SP 800-181, the NICE Cybersecurity Workforce Framework for a description of the specific role ID to include the Knowledge, Skills, Abilities (KSA) and Task associated with the role.
- **Step 3:** For the training under evaluation, collect all available descriptive information such as a course summary, outline, syllabus, and learning objectives, and keynote summaries that cover your Role-based training ID description. You may want to match up, KSAs and Tasks defined by your role to the course contents listed above to see if the training attended meets the annual role-based requirement.
- **Step 4:** Determine if the training description addresses some of the KSAs and Tasks associated with the desired NICE role.

The RBT Self-Assessment table, Figure 1, can be used as a guide to help determine if a training course/event meets the role-based training requirement. For example, measuring, or characterizing, the NICE Role ID's associated description, KSA, Task and/or role descriptions

[5] https://csrc.nist.gov/publications/detail/sp/800-181/final

against the training description. This will enable confirmation that a selected training event is relevant to the role-based training requirement.

Training Title	NICE Role ID:	Identify Relevance to NICE ID:				
		Role Description	Knowledge	Skills	Abilities	Tasks

Figure 1: RBT Self-Assessment Table

Personnel wishing to receive credit, for any form of RBT taken from an organization external to CMS, in satisfaction of any CMS training requirement, to first seek review and approval from their supervisor (or for Contractors, from their employer).

CMS provides role-based training to federal employees identified with SSR, including managers, senior executives, that is delivered through the Computer Based Training (CBT) system. The following steps detail CMS' process for this role-based training.

Initial Certification:

- **Step 1:** The Program notifies federal employees with SSR of the availability of CBT-based role-based training.
- **Step 2:** The employee logs into the CBT system and completes the RBT.
- **Step 3:** Once RBT is completed, the CBT system records the completion. An option to print the completion certificate is available, but it is not required.

After this Initial Certification, for new federal employees, the following steps will be followed:

- **Step 1:** On the Employee Entry of Duty (EOD), the User receives a CMS user ID activation Welcome email from Enterprise User Administration (EUA). Users are given seven (7) calendar days to complete RBT.
    - EUA sends reminder emails on a daily basis until certification is complete.
- **Step 2:** The User logs in to the CBT system and completes the RBT.
- **Step 3:** Once RBT is completed, the CBT system records training completions. An option to print the completion certificate is available, but it is not required.

Recertification:

- **Step 1:** Recertification is to be completed annually on the User ID activation month. The EUA system sends an email notification to the user at forty-five (45) days in advance of the recertification due date.
    - Email reminders to complete recertification are sent at 15, 10, 5, 4, 3, 2, and 1 day(s) until revocation date.
- **Step 3:** The User logs in to the CBT system and completes the RBT.

- **Step 4:** If the User does not complete the training within the recertification timeframe, revocation occurs the 1st day of the following month.

While Contractors are responsible for ensuring that that their personnel who have significant information privacy and security responsibilities have training commensurate with their role, they may request a copy of this CMS training course for use in their role-based training program.

6.3 Security Training Records (AT-4)

The purpose of Security Training Records is to document and monitor individual information system security and privacy training activities. Training activities include basic security and privacy awareness and training and specific role-based information system security and privacy training. Maintaining security and privacy training records provides the capability for organizations to track compliance with privacy-related training requirements. CMS retains individual training records for a minimum of five (5) years after the individual completes each training.

The table below outlines the CMS organizationally defined parameters (ODPs) for AT-4.

Table 3: CMS Defined Parameters – Control AT-4

Control	Control Requirement	CMS Parameter
AT-4	The organization: b. Retains individual training records for [Assignment: organization-defined time period].	The organization: c. Retains individual training records for a minimum of five (5) years after the individual completes each training.

Federal employee training records must be submitted and tracked with the respective Business Owners upon commencement of work and annually or upon request. Training requirements are based upon a cycle that begins on October 1 of the current year and ends on September 30 of the subsequent year.

Specialized role-based training verification includes:

- EUA ID
- Name of individual
- Assigned NICE role ID(s)
- Title of training
- Training description
- Date of training
- Entry of Duty date
- Exit of Duty date

It is recommended that federal employees use the CMS CBT to record training completions that are not provided and automatically recorded by the CBT. The following steps detail the process of submitting training information for employees:

- **Step 1:** Log in to www.cms.gov/cbt

- **Step 2:** Click on "Manage Training Information".
  Step 3: In the Reporting form, complete the fields in the appropriate sections for CMS provided training and any other additionally completed training.

Business Owners may request CBT training records for its personnel from the Program for tracking purposes.

Contractor training records must be submitted and tracked with the respective Contracting Officer (CO), or Contracting Officer's Representative (COR), upon commencement of work and quarterly thereafter or upon request. Training requirements are based upon a cycle that begins on October 1 of the current year and ends on September 30 of the subsequent year.

The following steps detail the process of submitting training information for contractors:

- **Step 1:** Using the Contractor Role Based Training Report Template (Report worksheet) in Appendix F, enter the applicable information. See Figure 2 for example of requested information.
- **Step 2:** Using the Contractor Role Based Training Report Template (Attestation worksheet) in Appendix F, complete the attestation confirming the completeness and accuracy of the report submission. See Figure 3.
- **Step 3:** The Contractor submits the completed Role Based Training Report Template spreadsheet to its CO or COR each calendar quarter as follows: on or before March 10, June 10, September 10 and December 10, or upon request.
- **Step 4:** The COR uploads the completed Role Based Training Report Template to the CBT, each calendar quarter as follows: on or before, March 15, June 15, September 15 and December 15, or upon request from the Program.

	A	B	C	D	E	F	G	H	I	J
1	**Role Based Training Report Template**									
2	**Contractor:** _____									
3	**Report Date:** _____									
4	**EUA ID**	**First Name**	**Last Name**	**NICE Role ID(s)**	**Title of Training(s)**	**Short Description of Training(s)**	**Date of Training (s)**	**Entry of Duty Date**	**Exit of Duty Date**	**Meets Annual or EoD Requirement? Y/N**
5	XYZ1	Fname1	Lname1	123, 233, 231	CAP CEH	Certified Authorization Professional CEH	10/03/2018, 10/15/2018	10/03/2018		Y
6										
7										
8										
9										
10										

Figure 2: Contractor RBT Report

	A	B	C	D	E	F	G	H	I	J	K
1	**Attestation**										
2											
3	On behalf of the Organization named below:										
4	I hereby attest that all staff members assigned to CMS have completed all required Role Based security and privacy training,										
5	and that this RBT Report is complete and accurate.										
6	By entering the information below, I declare that the above statement is true and accurate to the best of my knowledge.										
7											
8											
9	Enter Organization Name										
10	Enter Contract Number										
11	Enter Your Name										
12	Enter Date										

Figure 3: Contractor RBT Report Attestation

Appendix A. Acronyms

Selected acronyms used in this document are defined below.

Acronyms	Terms
ARS	Acceptable Risk Safeguards
CBT	Computer-based Training
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
EUA	Enterprise User Administration
HHS	Health and Human Services
ISPG	Information Security and Privacy Group
NIST	National Institute of Standards and Technology
POC	Point of Contact
RMH	Risk Management Handbook
SP	Special Publication
SSR	Significant Security and Privacy Responsibilities
SU	System User
UID	User ID

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.
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
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.
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).
Enterprise User Administration	Manages the CMS user identifications. For more detail see https://portal.cms.gov/wps/portal/unauthportal/faq
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

Terms	Definitions
	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, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. Also, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Office of Management and Budget	The Office of Management and Budget (OMB) designated the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) as authorities to provide guidance to federal agencies for implementing information security and privacy laws and regulations, including FISMA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974 ("Privacy Act"). This Policy addresses CMS applicable information security and privacy requirements arising from federal legislation, mandates, directives, executive orders, and Department of Health and Human Services (HHS) policy by integrating NIST SP-800-53v4, Security and Privacy Controls for Federal Information Systems and Organizations, with the Department of Health and Human Services Information Systems Security and Privacy Policy (IS2P) and specific programmatic legislation and CMS regulations. Appendix B lists these authoritative references.

Terms	Definitions
Risk Management Handbook	The Risk Management Handbook (RMH) compiles CMS standards, requirements, directives, practices, and procedures for protecting CMS information and information systems.
Significant Security and Privacy Responsibilities	Significant information security and privacy responsibilities will be defined by CMS as "the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the privacy or security posture of one or more HHS or CMS systems."
Training	Informing personnel of roles and responsibilities within a particular IT plan and teaching personnel skills related to those roles and responsibilities.

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., Statutes 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

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

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

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

Executive Order 13587 (Insider Threat Compliance)
https://it.ojp.gov/PrivacyLiberty/authorities/executive-orders#13587

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

E-Government Act of 2002 (Pub. L. No. 107-347) § 208
https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html

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

OMB Circular A-130 Management of Federal Information Resources
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
http://www.whitehouse.gov/omb/memoranda_m03-22/

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

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

NIST SP 800-12 *An Introduction to Information Security*
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

NIST SP 800-16 *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program*
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

NIST SP 800-100 *Information Security Handbook: A Guide for Managers*
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

NIST SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems*
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

NIST SP 800-53-r4, *Security and Privacy Controls for Federal Information Systems and Organizations*
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

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

C.5 HHS Policy

HHS Memorandum: *Requirements for Role-Based Training (RBT) of Personnel with Significant Security Responsibilities*
https://intranet.hhs.gov/it/strategy-policy-governance/policies-standards-guides/memoranda/role-based-training-personnel-ssrmemorandum-2017.pdf (Intranet Only)

HHS-OCIO-2014-0001 *HHS Information System Security and Privacy Policy (HHS IS2P)*
HHS Information Security and Privacy Policy (IS2P) – 2014 Edition. If you are having a problem obtaining a copy of this document, please email fisma@hhs.gov

HHS- OCIO 2018-0004 *HHS Rules of Behavior for Use of HHS Information and IT Resources Policy*
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/HHS-Rules-of-Behavior-for-Use-of-HHS-Information-and-IT-Resources-Policy.html?DLPage=1&DLEntries=10&DLFilter=rules&DLSort=0&DLSortDir=ascending

C.6 CMS Policy and Directives

CMS Information Systems Security and Privacy Policy (IS2P2)
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS2P2.pdf

CMS Office of Acquisition and Grants Management (OAGM)
https://www.cms.gov/About-CMS/Leadership/oagm

C.7 Associated CMS Resources

ISPG Training Catalog
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ISPG-Training-Catalog.html?DLPage=1&DLEntries=10&DLFilter=training&DLSort=0&DLSortDir=ascending

Computer Based Training (CBT)
www.cms.gov/cbt

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

Appendix D. CMS NICE Role Education Course Mapping Guide

The RMH Chapter 02 Awareness and Training Appendix D: CMS NICE Role Education Course Mapping Guide 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/Downloads/ISPG-Training-Catalog.pdf

Appendix E. Cybersecurity & Privacy Training Catalog

The RMH Chapter 02 Awareness and Training Appendix E: Cybersecurity & Privacy Training Catalog 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/Info-Security-Library-Items/ISPG-Training-Catalog.html?DLPage=1&DLEntries=10&DLFilter=training&DLSort=0&DLSortDir=ascending

Appendix F. Role-Based Training Report Template

The RMH Chapter 02 Awareness and Training Appendix F Role-Based Training Report Template is available within the CMS CBT located at:

https://www.cms.gov/cbt/login/default.aspx

Appendix G. Points of Contact

ISPG Training Team

Name	Email
ISPG	CMSISPGTrainers@cms.hhs.gov

Appendix H. 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.