CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF ENTERPRISE INFORMATION

Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Risk Management Handbook (RMH)
Chapter 8: Incident Response

Final

Version 1.0

January 31, 2017

Record of Changes

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

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
1.0	01/31/2017	All	CMS ISPG	Initial Publication

Effective Date/Approval

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becomes effective on the date that CMS’s Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified, or superseded by another policy.

Signature: /s/ Date of Issuance: 1/31/2017

George Hoffman
Acting Chief Information Officer
and Director, Office of Enterprise
Information (OEI)

Policy Owner’s Review Certification

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

Signature: ______________________ Date of Annual Review: ____________

Emery Csulak
CMS Chief Information Security Officer
and Senior Official for Privacy

Table of Contents

1. Purpose 7

1.1 Authority 7
1.2 Scope 7
1.3 Handbook Structure 8
1.4 Background 9
1.5 Policy 11
1.6 Standards 12
1.7 Guidelines 12

2. Roles and Responsibilities 13

3. Procedures 14

3.1 Incident Response Training (IR-02) 14
3.1.1 Simulated Events (IR-02(01)) 15
3.1.2 Automated Training Environments (IR-02(02)) 16
3.2 Incident Response Testing (IR-03) 17
3.2.1 Automated Testing (IR-03(01)) 18
3.2.2 Coordination with Related Plans (IR-03(02)) 18
3.3 Incident Handling (IR-04) 19
3.3.1 Preparation 20
3.3.2 Detection and Analysis 22
3.3.3 Containment, Eradication and Recovery 27
3.3.4 Post-Incident Activity 28
3.3.5 Automated Incident Handling Processes (IR-04(01)) 28
3.3.6 Continuity of Operations (IR-04(03)) 29
3.3.7 Insider Threats-Intra-Organizations (IR-04(07)) 30
3.3.8 Correlation with External Organizations (IR-04(08)) 31
3.4 Incident Monitoring (IR-05) 32
3.4.1 Automated Tracking/Data Collection/Analysis (IR-05(01)) 32
3.5 Incident Reporting (IR-06) 33
3.5.1 Automated Reporting (IR-06(01)) 34
3.6 Incident Response Assistance (IR-07) 35
3.6.1 Automation Support for Availability of Information/Support (IR-07(01)) 35
3.6.2 Coordination with External Providers (IR-07(02)) 35
3.7 Incident Response Plan (IR-08) 36
3.8 Information Spillage Response (IR-09) 37
3.8.1 Information Spillage Response/Responsible Personnel (IR-09(01)) 39
3.8.2 Information Spillage Response/Training (IR-09(02)) 39
3.8.3 Post-Spill Operations (IR-09(03)) 39
3.8.4 Exposure to Unauthorized Personnel (IR-09(04)) 40
3.9 Integrated Information Security Analysis Team (IR-10) 41

Appendix A. Acronyms ... 42

Appendix B. Glossary of Terms ... 46

Appendix C. Applicable Laws and Guidance ... 59

Appendix D. ARS Standards – Incident Response (IR) ... 65

Appendix E. Control/Policy Cross Reference Table ... 83

Appendix F. Impact Classifications & Threat Vectors Descriptions ... 86

Appendix G. Tabletop Exercise Test Plan Template ... 88

Appendix H. Tabletop Exercise Participant Guide Template ... 91

Appendix I. After Action Report ... 93

Appendix J. Incident Scenarios ... 96

Appendix K. Incident Response Reporting Template ... 101

Appendix L. Incident Response Plan Template ... 103

Appendix M. Incident Preparation Checklist ... 112

Appendix N. Points of Contact ... 115

Appendix O. Feedback and Questions ... 116

Tables

Table 1: CMS Defined Parameters – Control IR-2 ... 15

Table 2: CMS Defined Parameters – Control IR-3 ... 17

Table 3: Common Sources of Precursors and Indicators ... 23

Table 4: Automated Tools ... 29

Table 5: CMS Defined Parameters - Control IR-4(03) ... 29

Table 6: CMS Defined Parameters - Control IR-04(07) ... 30

Table 7: CMS Defined Parameters - Control IR-4(08) ... 31

Table 8: CMS Defined Parameters – Control IR-6 ... 33

Table 9: CMS Defined Parameters - Control IR-8 ... 36

Table 10: CMS Defined Parameters - Control IR-9 ... 38

Table 11: CMS Defined Parameters - IR-9(02) 39
Table 12: CMS Defined Parameters - IR-9(03) 40
Table 13: CMS Defined Parameters - IR-9(04) 40

Figures

Figure 1: CCIC Functional Areas Overview 10
Figure 2: Incident Response Life Cycle 19

1. Purpose

The Centers for Medicare and Medicaid Services (CMS) *RMH Chapter 8 Incident Response* is written in compliance with the *CMS Information Systems Security and Privacy Policy (IS2P2)* and the *CMS Information Security Acceptable Risk Safeguards (ARS)*. The intent of this document is to describe standard operating procedures that facilitate the implementation of security controls associated with the Incident Response (IR) family of controls taken from the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations* and tailored to the CMS environment in the CMS ARS.

1.1 Authority

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

Per the Department of Health and Human Services (HHS) Information Systems Security and Privacy Policy, 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 policy also designates the Senior Official for Privacy (SOP) as the CMS authority for implementing the CMS-wide privacy program. Through this Policy, the CIO/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 this handbook to ensure compliance with federal requirements and programmatic policies, standards, procedures, and to facilitate the implementation of information security and privacy controls.

1.2 Scope

This handbook documents the procedures that facilitate the implementation of the security controls and standards defined in the CMS IS2P2[1] and the CMS ARS[2] for the IR family of security controls. This handbook is 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 other applicable law, higher-level agency directive, or existing

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

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

labor management agreement in place. This handbook replaces CMS RMH Volume III Standard 7-1 Incident Handling.

1.3 Handbook Structure

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

This document is organized by sections and appendices as follows:

- **Purpose**
    - Authority
    - Scope
    - Handbook Structure
    - Background
    - Policy
    - Standards
    - Guidelines
- **Roles and Responsibilities**
- **Procedures**
- **Appendices**
    - Appendix A: Acronyms
    - Appendix B: Glossary of Terms
    - Appendix C: Applicable Laws and Guidance
    - Appendix D: ARS Standards – Incident Response (IR)
    - Appendix E: Control/Policy Cross Reference Table
    - Appendix F: Impact Classifications and Threat Vectors Descriptions
    - Appendix G: Tabletop Exercise Test Plan Template
    - Appendix H: Tabletop Exercise Participant Guide Template
    - Appendix I: After-Action Report
    - Appendix J: Incident Scenarios

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

- Appendix K: Incident Response Reporting Template
- Appendix L: Incident Response Plan Template
- Appendix M: Incident Preparation Checklist
- Appendix N: Points of Contact
- Appendix O: Feedback and Questions

1.4 Background

NIST 800-53r4 states under the IR control family that an organization develops, disseminates, and must periodically review and update its incident response documentation. This includes a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

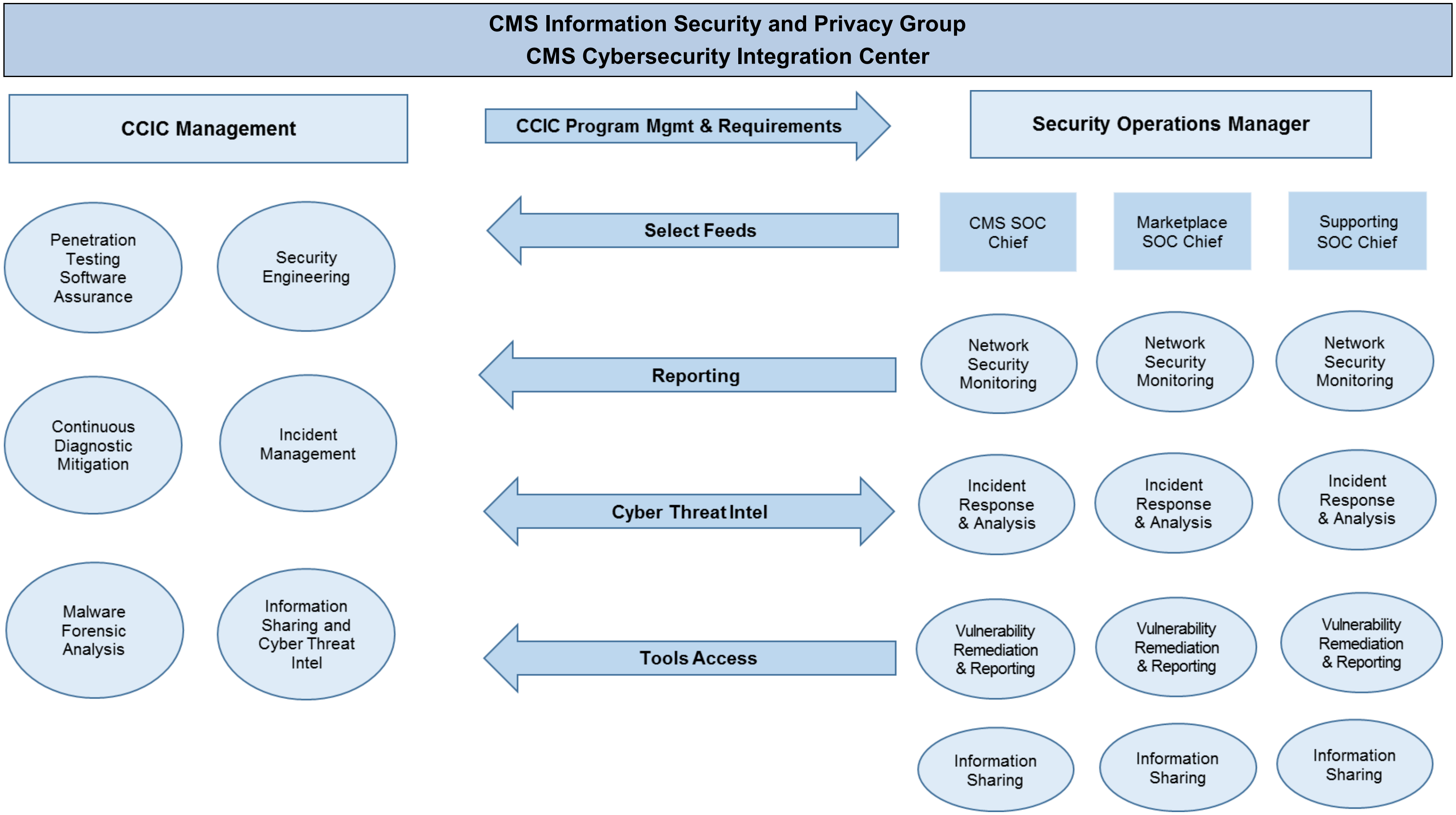
This *RMH Chapter 8: Incident Response* provides procedures to assist with the implementation of the IR family of controls to ensure incident response for FISMA systems within the CMS enterprise environment and on any systems storing, processing, or transmitting CMS information on behalf of CMS. This control family addresses the establishment of policy and procedures for the effective implementation of selected security and privacy controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

For purposes of incident response and handling, the CMS Cybersecurity Integration Center (CCIC) integrates an Incident Management Team (IMT). This team ensures that incident response processes and procedures are followed, and provides direction and support to all CMS components and contractors conducting corrective actions to mitigate information security and privacy incidents.

Reportable events and high impact incidents are to be reported to the IMT via the CMS IT Service Helpdesk who will open a CMS Remedy ticket, which then creates a shell ticket in Risk Vision for HHS.

Figure 1 below outlines the CCIC Functional Areas Overview.

Figure 1: CCIC Functional Areas Overview


CMS Information Security and Privacy Group
CMS Cybersecurity Integration Center
CCIC Management
CCIC Program Mgmt & Requirements
Security Operations Manager
Select Feeds
CMS SOC Chief
Marketplace SOC Chief
Supporting SOC Chief
Penetration Testing Software Assurance
Security Engineering
Reporting
Network Security Monitoring
Network Security Monitoring
Network Security Monitoring
Continuous Diagnostic Mitigation
Incident Management
Cyber Threat Intel
Incident Response & Analysis
Incident Response & Analysis
Incident Response & Analysis
Malware Forensic Analysis
Information Sharing and Cyber Threat Intel
Tools Access
Vulnerability Remediation & Reporting
Vulnerability Remediation & Reporting
Vulnerability Remediation & Reporting
Information Sharing
Information Sharing
Information Sharing

1.5 Policy

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

- IR-1 The Program must develop and maintain the IR family of controls to establish an operational incident handling capability for information systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Incidents must be tracked, documented, and reported. The Program must:
  - IR-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the IR family of controls in the ARS to:
    - IR-1.1.1 Document, maintain, and communicate policies and procedures in accordance with the HHS Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response and the HHS Policy for Responding to Breaches of PII, including roles and responsibilities for information security and PII incidents and violation handling
    - IR-1.1.2 Ensure CMS and contractor situational awareness through:
      - IR-1.1.2.1 Receipt of information system security and privacy alerts, advisories, and directives from designated external organizations on an ongoing basis
      - IR-1.1.2.2 Generation of internal information security and privacy alerts, advisories, and directives as deemed necessary
      - IR-1.1.2.3 Dissemination of information security and privacy alerts, advisories, and directives to personnel (see the ARS for a complementary, CMS-defined process)
    - IR-1.1.3 Ensure CMS and contractor awareness of privacy-related incidents through:
      - IR-1.1.3.1 Development and implementation of privacy breach notification and response policies, processes, and standards
      - IR-1.1.3.2 Appropriate notification of the SOP for all incidents involving PII or PHI
    - IR-1.1.4 Ensure CMS and contractors maintain incident response processes and procedures by:
      - IR-1.1.4.1 Reviewing and updating Incident Response Plans periodically as defined in the ARS
      - IR-1.1.4.2 Testing Incident Response Plans periodically as defined in the ARS
      - IR-1.1.4.3 Incorporating lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises

  - IR-1.1.5 Ensure CMS and contractors maintain familiarity with incident response processes and procedures through periodic training, as defined in the ARS
- IR-1.2 The CMS CISO, in coordination with the CMS Director of CCIC and Business Owners/Information System Owners (ISOs), must establish and maintain an information security and privacy incident and breach response capability that includes preparation, identification, containment, eradication, recovery, and follow-up capabilities to ensure effective recovery from information security and privacy incidents and breaches:
  - IR-1.2.1 For systems categorized as “Moderate” or “High” under Federal Information Processing Standard (FIPS) 199, incident handling activities must be coordinated with contingency planning activities
  - IR-1.2.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Incident Response family of controls

CMS IS2P2 defines the framework and policy under which CMS protects and controls access to CMS information and information systems in compliance with HHS policy and federal law. The “Procedures” section of this handbook outlines the specific processes for meeting the IR security control requirements as required by the CMS IS2P2 and the CMS ARS. These procedures have been tailored based on the current CMS implementation of these documents.

1.6 Standards

Standards consist of specific security control implementation requirements that enforce and support the information security policy. The CMS ARS defines CMS specific standards for each of the required NIST SP 800-53r4 security controls in compliance with HHS policy and the CMS IS2P2. The CMS ARS standards for the IR family of controls are outlined in Appendix D.

1.7 Guidelines

Guidelines provide direction and best practices that help support the standards or serve as a reference when no standard exists. Guidelines provide guidance and best practices relative to a particular topic. Guidelines may accompany, interpret, or provide guidance for implementing CIO policies, or may provide guidance to various CMS IT Life Cycle activities. Guidelines are recommended best practices but are not required to comply with policy. A guideline aims to streamline particular processes according to a set routine or sound practice.

The list below contains some examples of CMS guidelines for the IR family:

- NIST SP 800-61 Rev. 2: *Computer Security Incident Handling Guide* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST SP 800-84: *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* http://dx.doi.org/10.6028/NIST.SP.800-85A-4
- US-CERT: *United States Computer Emergency Readiness Team* https://www.us-cert.gov/

2. Roles and Responsibilities

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

- HHS Chief Information Officer (CIO)
- HHS Chief Information Security Officer (CISO)
- HHS Computer Incident Response Center (CSIRC)
- HHS/OIG Computer Crime Unit (CCU)
- HHS Privacy Incident Response Team (PIRT)
- CMS Chief Information Officer (CIO)
- CMS Chief Information Security Officer (CISO)
- CMS Information System Security Officer (ISSO)
- CMS Cyber Risk Advisor (CRA)
- CMS Information Security and Privacy Group (ISPG)
- CMS Cybersecurity Integration Center (CCIC)
- CMS IT Service Desk
- CMS Senior Official for Privacy (SOP)
- CMS Business Owner (BO)
- CMS Federal Employee and Contractors
- CMS Data Guardian

3. Procedures

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

3.1 Incident Response Training (IR-02)

The purpose of Incident Response Training is to prepare individuals to prevent, detect, and respond to security and privacy incidents, and ensure that CMS fulfills FISMA requirements. Incident response training should be consistent with the roles and responsibilities assigned in the incident response plan. For example, incident response training is applicable to System Owners (SO), Information Owners, and Information System Security Officers (ISSO). CMS personnel (i.e., employees and contractors) who routinely access sensitive data, such as names, Social Security numbers, and health records in order to carry out the CMS mission receive incident response training annually as part of the general information security awareness training.

The CIO, CISO, and the SOP shall endorse and promote an organizational-wide information systems security and privacy awareness training. According to CMS IS2P2 Section 2.2, the CMS Chief Information Officer (CIO), shall establish, implement, and enforce a CMS-wide framework to facilitate an incident response program including Personal Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI) breaches that ensures proper and timely reporting to HHS. In the CMS IS2P2 Section 2.3, the CMS Chief Information Security (CISO) shall ensure the CMS-wide implementation of Department and CMS policies and procedures that relate to information security and privacy incident response.

Users must be aware that the Internal Revenue Code (IRC), Section 6103(p) (4) (D) requires that agencies receiving Federal Tax Information (FTI) provide appropriate safeguard measures to ensure the confidentiality of the FTI. Incident response training is one of the safeguards for implementing this requirement. For a definition of FTI, review Appendix B Glossary of Terms.

The CMS Information Security and Privacy Group (ISPG) will provide incident response training to information system users which is consistent with assigned roles and responsibilities when assuming an incident response role or responsibility and annually thereafter. For example, general users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. In addition, those responsible for identifying and responding to a security incident must understand how to recognize when PII or PHI are involved so that they can coordinate with the designated privacy official.

The table below outlines the CMS organizationally defined parameters (ODPs) for IR training.

Table 1: CMS Defined Parameters – Control IR-2

Control	Control Requirement	CMS Parameter
IR-2	The organization provides incident response training to information system users consistent with assigned roles and responsibilities:	
	a. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility;	a. Within one (1) month of assuming an incident response role or responsibility
	b. When required by information system changes; and	b. N/A – no Organizational Defined Parameters (ODPs)
	c. [*Assignment: organization-defined frequency*] thereafter	c. At least once every 365 days thereafter

Training for General Users

For all Enterprise User Administration (EUA) users the following steps outline the process for completing the CMS Computer-based Training (CBT), which includes IR training.

- **Step 1:** The incident response training is incorporated into the annual Security and Privacy Awareness Training. All EUA users must take the CBT Training located at https://www.cms.gov/cbt/forms/isspa.aspx. The training must be delivered to all EUA users initially prior to account issuance and annually thereafter
- **Step 2:** Each year based on the date of account issuance each user receives an email that requires a review and completion of the annual CBT
- **Step 3:** Training records are maintained using the CBT database and include the User ID (UID) and the date the individual last completed the training

Role-based Training

For individuals with incident response roles and responsibilities, role-based training is satisfied through the execution of a tabletop exercise as long as all personnel with incident response roles and responsibilities participate in the exercise. Review Section 3.2 Incident Response Testing for procedures to conduct a tabletop exercise.

3.1.1 Simulated Events (IR-02(01))

The purpose of this control is to facilitate the effective response by personnel who handle crisis situations by incorporating simulated events into incident response training. Exercises involving simulated incidents can also be very useful for preparing staff for incident handling.[4]

The selection of the scenarios should occur as a part of the test plan development; see Section 3.2 Incident Response Testing for developing the test plan. The following details the CMS specific

[4] See NIST SP 800-84 – *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf and NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

process for incorporating simulated events/scenarios into incident response training, through the execution of a tabletop exercise.

- **Step 1:** Select two scenarios from the list below which will form the foundation of the tabletop exercise. Document the scenarios and a description of each in the Tabletop Exercise Test Plan. It is important to select your scenarios based upon an assessment of risk (i.e., the greatest current threats). Weaknesses identified during prior incidents might identify good candidate scenarios for future incident response tests. In addition, results from prior security control assessments (SCAs) or existing Plan of Action and Milestones (POA&Ms) might assist in selecting scenarios for incident response testing. For example, if access control was identified as a weakness during a prior SCA, a good scenario to select for incident response testing would be scenario 6 (Unauthorized Access to Payroll Records). Appendix J contains detailed descriptions for each of the scenarios listed below:
    - **Scenario 1:** Domain Name System (DNS) Server Denial of Service (DoS)
    - **Scenario 2:** Worm and Distributed Denial of Service (DDoS) Agent Infestation
    - **Scenario 3:** Stolen Documents
    - **Scenario 4:** Compromised Database Server
    - **Scenario 5:** Unknown Exfiltration
    - **Scenario 6:** Unauthorized Access to Payroll Records
    - **Scenario 7:** Disappearing Host
    - **Scenario 8:** Telecommuting Compromise
    - **Scenario 9:** Anonymous Threat
    - **Scenario 10:** Peer-to-Peer File Sharing
    - **Scenario 11:** Unknown Wireless Access Point
- **Step 2:** Ensure that the material developed for the tabletop exercise supports the scenarios selected. Review Section 3.2 Incident Response Testing for more information for developing the exercise material
- **Step 3:** Execute the tabletop test using the procedures outlined below in Section 3.2 Incident Response Testing

3.1.2 Automated Training Environments (IR-02(02))

The purpose of Incident Response Training/Automated Training Environments is to ensure that CMS employs automated mechanisms to provide a more thorough and realistic incident training environment. At CMS, incident training and incident response testing are both satisfied through the execution of a tabletop exercise. These tabletop exercises are designed to incorporate automated mechanisms for incident response, review Section 3.2.1 Automated Testing for detailed procedure which ensure automated mechanisms are incorporated into incident response training.

3.2 Incident Response Testing (IR-03)

The purpose of the Incident Response Testing is to ensure that CMS tests the incident response capability for the information system using testing principles to determine the incident response effectiveness and document the results.

The table below outlines the CMS organizationally defined parameters (ODPs) for IR testing.

Table 2: CMS Defined Parameters – Control IR-3

Control	Control Requirement	CMS Parameter
IR-3	The organization tests the incident response capability for the information system: [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results	Annually, tabletop testing, checklists; walk-through, discussion-based, or tabletop exercises; comprehensive, functional exercises executed in a simulated operational environment; and documents results for assessment and potential process improvement

CMS incident response testing is accomplished through the execution of tabletop exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss roles during an emergency and the responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

The following steps detail the CMS specific process for conducting a tabletop exercise:

- **Step 1:** Complete the Test Plan utilizing the Tabletop Exercise Test Plan Template provided in Appendix G**.** Testing must include two scenario-based exercises to determine the ability of the CMS to respond to information security and privacy incidents. Scenarios should be selected which integrate the use of automated mechanisms for incident response. Review Section 3.1.1 Simulated Events for example scenarios and Section 3.2.1 Automated Testing for procedures for integrated automated mechanisms into the tabletop exercise

- **Step 2:** Acquire approval of the Test Plan from the Business Owner and/or ISSO. The approval is granted by signing the final row of the Test Plan

- **Step 3:** Develop the exercise materials (e.g., briefings, Participant Guide). A sample Tabletop Exercise Participant Guide Template is shown in Appendix H. For more information on functional exercise material please refer to Section 5.3 of NIST Special

Publication 800-84**,** *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

- **Step 4:** Conduct the tabletop exercise according to the approved Test Plan. The agenda contained within the Test Plan serves as a guide for executing the exercise. Prior to releasing the exercise participants, the Exercise Facilitator and Data Collector conduct a debrief/hotwash
- **Step 5:** Evaluate the tabletop exercise by completing the After-Action Report located in Appendix I. This step is completed by the Exercise Facilitator and Data Collector

3.2.1 Automated Testing (IR-03(01))

The purpose the Incident Response Testing/Automated Testing is to ensure that CMS employs automated mechanisms to more thoroughly and effectively test the incident response capability. The following steps detail the CMS specific process to ensure that automated mechanisms have been incorporated into testing:

- **Step 1:** Ensure that the scenarios selected in the test plan incorporate the use of automated incident response tools, and complete prior to test plan approval. For example, the review of audit logs using the CMS audit reduction tool (Splunk) or the creation of a ticket for tracking an incident using the Agency's tool (RiskVision). Review Table 4 in Section 3.3.5 Automated Incident Handling Processes for a list of automated tools used to support the incident response capability
- **Step 2:** Ensure that the tabletop exercise material contains content on the use of automated mechanism. For example, inserting screen shots demonstrating how to generate a RiskVision ticket, or a walkthrough of how to use the Splunk audit reduction capability
- **Step 3:** Execute the tabletop test using the procedures outlined in Section 3.2 Incident Response Testing

3.2.2 Coordination with Related Plans (IR-03(02))

The purpose of the Incident Response Testing/Coordination with Related Plans is to ensure that CMS coordinates incident response testing with organizational elements responsible for related plans. Related plans can include but are not limited to the following:

- Configuration Management Plan
- Information System Contingency Plan
- Patch and Vulnerability Management Plan
- Information System Continuous Monitoring Strategy/Plan

The following steps detail the CMS specific process to ensure Coordination with Related Plans:

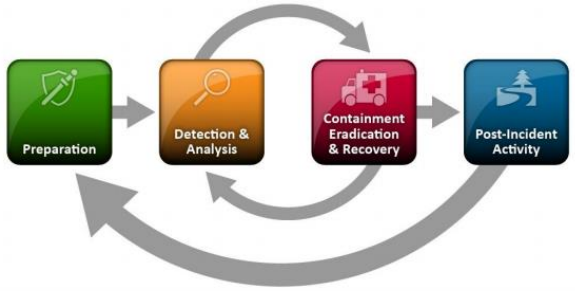
- **Step 1:** Identify the related plans and the stakeholders associated with each
- **Step 2:** Establish a primary method of communication. Possible methods of communication include emails, face-to-face meetings, and teleconferences

- **Step 3:** Using the primary method of communication identified above, request copies of related plans. Review the related plans identifying dependencies for the IR test
- **Step 4:** Identify stakeholders from related plans that will be required to participate in the incident response exercise. Coordinate with the stakeholders through the establishment, review and execution of a test plan
- **Step 5:** Conduct follow up communications as necessary. Specifically, a copy of the After-Action Report should be provided to stakeholders associated with related plans so that those plans may be updated as needed

3.3 Incident Handling (IR-04)

The purpose of this control is to ensure that CMS implements an incident handling capability for security and privacy incidents that includes 1) preparation, 2) detection and analysis, 3) containment, eradication, and recovery, and 4) post incident activity which are the four phases of the incident response lifecycle as demonstrated in the diagram below.

Figure 2: Incident Response Life Cycle



All distributed Incident Response Teams (IRT) fall under the authority of the CMS CCIC IMT, the single information security and privacy incident coordination entity. Each individual system is responsible for identifying incident responders as part of the system's Incident Response Plan (IRP). The incident responders serve as the frontline of the incident handling capability with oversight and incident response assistance provided by the IMT. This section of the document establishes the specific requirements and processes for maintaining a unified, cohesive incident handling capability across the CMS enterprise and describes the relationship between the IMT and the frontline incident responders.

Incident handling activities should be coordinated with contingency planning activities; and the lessons learned from ongoing incident handling activities should be incorporated into incident response procedures, training and testing. The procedure below provides an inclusive set of specific steps and requirements for handling information security and privacy incidents using the four-phase lifecycle. This lifecycle must be used by the IMT and the frontline incident responders to properly handle information security and privacy incidents.

3.3.1 Preparation

Incident response methodologies typically emphasize preparation, not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. The following steps detail the CMS specific process for phase one (preparation) of the incident handling lifecycle:

- **Step 1:** Ensure the proper preparations have been made to respond to information security and privacy incidents by completing the Incident Preparation Checklist located in Appendix M. This checklist should be reviewed annually in coordination with the update to the incident response plan
- **Step 2:** Ensure regular practices have been implemented to prevent information security and privacy incidents. The list below taken from NIST SP 800-61 Rev. 2 provides a brief overview of some of the main recommended practices for securing networks, systems, and applications:
    - **Risk Assessments:** Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources

      The CMS standard for risk assessment requires that the results of the risk assessment are reviewed at least annually and that the risk assessment is updated at least every three years or when a significant change occurs
    - **Host Security:** All hosts should be hardened appropriately using standard configurations. In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege, granting users only the privileges necessary for performing authorized tasks. Hosts should have auditing enabled and should log significant security-related events. The security of hosts and configurations should be continuously monitored. Many organizations use Security Content Automation Protocol (SCAP) configuration checklists to assist in securing hosts consistently and effectively

      The CMS standard requires the implementation of the latest security configuration baselines established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP)
    - **Network Security:** The network perimeter should be configured to deny all activity that is not expressly permitted. This includes securing all connection points, such as virtual private networks (VPNs) and dedicated connections to other organizations

The CMS standard requires that the information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception)

- **Malware Prevention:** Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients). The CMS standard requires that malicious code protection mechanisms are implemented as follows:

    - **Desktops:** Malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours

    - **Servers**(to include databases and applications)**:** Malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours

      In addition, malicious code protection mechanisms should be updated whenever new releases are available in accordance with CMS configuration management policy and procedures. Antivirus definitions should be updated in near-real-time. Malicious code protection mechanisms should be configured to lock and quarantine malicious code and send alerts to administrators in response to malicious code detection

- **User Awareness and Training:** Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications as well as the policy and procedures for safeguarding data that is not in digital form (e.g. PII in paper form). Applicable lessons learned from previous incidents should also be shared with users to evaluate how actions taken by the user could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents. IT staff should be trained to maintain networks, systems, and applications in accordance with the organization’s security standards. All users should be trained to protect printed hard/paper copies of data, including PII

  The CMS standard requires all general users receive security and privacy awareness training annually. The incident response training is incorporated into the annual Security and Privacy Awareness Training. All EUA users must take the CBT Training located at https://www.cms.gov/cbt/forms/isspa.aspx. The training must be delivered to all EUA users initially prior to account issuance and annually thereafter

- **Maintain Inventory:** Maintain an accurate inventory of information system components identifying those components that store, transmit, and/or process PII. An accurate inventory facilitates the implementation of the appropriate information security and privacy controls and is critical to preventing, detecting and responding to information security incidents

- **Step 3:** Ensure that the preparation and prevention techniques listed in Steps 1 and 2 above have been incorporated into the incident response plan for the information system and exercised at least annually. Review Section 3.7 Incident Response Plan or details on developing the incident response plan and Section 3.2 Incident Response Testing for details on incident response testing

3.3.2 Detection and Analysis

- **Step 1:** Prepare for Common Attack Vectors. The attack vectors listed below are not intended to provide definitive classification for incidents; but rather, to simply list common methods of attack, which can be used as a basis for detection:
  - **External/Removable Media:** An attack executed from removable media or a peripheral device, for example, malicious code spreading onto a system from an infected universal serial bus (USB) flash drive
  - **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a Distributed Denial of Service (DDoS) intended to impair or deny access to a service or application; or a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures)
  - **Web:** An attack executed from a website or web-based application; for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware
  - **Email:** An attack executed via an email message or attachment; for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message
  - **Impersonation:** An attack involving replacement of something benign with something malicious; for example: spoofing, man in the middle attacks, rogue wireless access points, and structured query language (SQL) injection attacks all involve impersonation
  - **Improper Usage:** Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system

- **Step 2:** Recognize the Signs of an Incident. Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now. Precursors and indicators are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people. The table below, taken from NIST SP 800-61 Rev. 2, lists common sources of precursors and indicators for each category

Table 3: Common Sources of Precursors and Indicators

Source	Description
Alerts	
IDPSs	Intrusion Detection and Prevention Systems (IDPS) products identify suspicious events regarding record pertinent data, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives,* alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, and can generate alerts based on analysis of log data.
Antivirus and anti-spam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if signatures are kept up to date. Anti-spam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing checksum with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, little information is provided about the nature of the

Source	Description
	activity. Still, the devices can be valuable in identifying network trends and in correlating events detected by other devices.
Network flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Organizations such as US-CERT33 and CERT®/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information is the confidence of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking the other party's systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

- **Step 3:** Report and Analyze the Incident. Report the incident using the procedures outlined in Section 3.5 Incident Reporting. Once reported the IMT and frontline IR responders analyze the incident. The following are recommendations taken from NIST-SP 800-61 Rev. 4 *Computer Security Incident Handling Guide* for making incident analysis easier and more effective:
  - **Profile Networks and Systems**: Profiling is measuring the characteristics of expected activity so that changes to it can be more easily identified. Examples of profiling are running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. In practice, it is difficult to detect incidents accurately using most profiling techniques; organizations should use profiling as one of several detection and analysis techniques
  - **Understand Normal Behaviors**: Incident response team members should study networks, systems, and applications to understand what the normal behavior is so that

abnormal behavior can be recognized more easily. No incident handler will have a comprehensive knowledge of all behavior throughout the environment, but handlers should know which experts could fill in the gaps. One way to gain this knowledge is through reviewing log entries and security alerts. This may be tedious if filtering is not used to condense the logs to a reasonable size. As handlers become more familiar with the logs and alerts, handlers should be able to focus on unexplained entries, which are usually more important to investigate. Conducting frequent log reviews should keep the knowledge fresh, and the analyst should be able to notice trends and changes over time. The reviews also give the analyst an indication of the reliability of each source

- **Create a Log Retention Policy:** Information regarding an incident may be recorded in several places, such as firewall, IDPS, and application logs. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. Another reason for retaining logs is that incidents may not be discovered until days, weeks, or even months later. The length of time to maintain log data is dependent on several factors, including the organization’s data retention policies and the volume of data. See NIST SP 800-92, *Guide to Computer Security Log Management* for additional recommendations related to logging
- **Perform Event Correlation:** Evidence of an incident may be captured in several logs that each contain different types of data, firewall log may have the source IP address that was used, whereas an application log may contain a username. A network IDPS may detect that an attack was launched against a particular host, but it may not know if the attack was successful. The analyst may need to examine the host’s logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred
- **Keep All Host Clocks Synchronized**: Protocols such as the Network Time Protocol (NTP) synchronize clocks among hosts. Event correlation will be more complicated if the devices reporting events have inconsistent clock settings. From an evidentiary standpoint, it is preferable to have consistent timestamps in logs, for example, to have three logs that show an attack occurred at 12:07:01 a.m., rather than logs that list the attack as occurring at 12:07:01, 12:10:35, and 11:07:06
- **Maintain and Use a Knowledge Base of Information:** The knowledge base should include information that handlers need for referencing quickly during incident analysis. Although it is possible to build a knowledge base with a complex structure, a simple approach can be effective. Text documents, spreadsheets, and relatively simple databases provide effective, flexible, and searchable mechanisms for sharing data among team members. The knowledge base should also contain a variety of information, including explanations of the significance and validity of precursors and indicators, such as IDPS alerts, operating system log entries, and application error codes
- **Use Internet Search Engines for Research:** Internet search engines can help analysts find information on unusual activity. For example, an analyst may see some

unusual connection attempts targeting TCP port 22912. Performing a search on the terms "TCP," "port," and "22912" may return some hits that contain logs of similar activity or even an explanation of the significance of the port number. Note that separate workstations should be used for research to minimize the risk to the organization from conducting these searches

- **Run Packet Sniffers to Collect Additional Data:** Sometimes the indicators do not record enough detail to permit the handler to understand what is occurring. If an incident is occurring over a network, the fastest way to collect the necessary data may be to have a packet sniffer capture the network traffic. Configuring the sniffer to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other information. Because of privacy concerns, some organizations may require incident handlers to request and receive permission before using packet sniffers
- **Filter the Data:** There is simply not enough time to review and analyze all the indicators; at minimum, the most suspicious activity should be investigated. One effective strategy is to filter out categories of indicators that tend to be insignificant. Another filtering strategy is to show only the categories of indicators that are of the highest significance; however, this approach carries substantial risk because new malicious activity may not fall into one of the chosen indicator categories
- **Seek Assistance from Others:** Occasionally, the team will be unable to determine the full cause and nature of an incident. If the team lacks sufficient information to contain and eradicate the incident, then it should consult with internal resources (e.g., information security staff) and external resources (e.g., US-CERT, other CSIRTs, contractors with incident response expertise). It is important to accurately determine the cause of each incident so that it can be fully contained

- **Step 4:** Document the incident using the Incident Response Reporting Template form located in Appendix K

- **Step 5:** Prioritize the incident using the criteria located in Appendix F Impact Classifications and Threat Vectors Descriptions

- **Step 6:** Establish communication method and notify the appropriate individuals. The list below provides examples of individuals that may require notification in the event of an incident:

  - CIO
  - CISO
  - Deputy CISO
  - SOP
  - HHS
  - ISSO
  - Local information response team within the organization
  - External incident response team (if appropriate)
  - System Owner
  - Human resources (for cases involving employees, such as harassment through email)

- Finance/Acquisition (in the case where extra finding is needed for investigation activities)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- US-CERT (required for Federal agencies and systems operated on behalf of the Federal government
- Law enforcement (if appropriate)
- Individual (whose PII has been compromised)

3.3.3 Containment, Eradication and Recovery

- **Step 1:** Choose a containment strategy. The containment strategy is determined based on the type of the incident (e.g., disconnect system from the network, or disable certain functions). Frontline incident responders should work with the IMT to select an appropriate containment strategy

- **Step 2:** Gather and handle evidence. The CCIC Forensic, Malware and Analysis Team (FMAT) maintain the criteria for evidence collection and a procedure to ensure a chain of custody. The IMT will coordinate with the FMAT to provide incident responders with assistance to collect and handle evidence

- **Step 3:** Identify the attacking host. The following items taken from NIST-SP 800-61 Rev. 4 *Computer Security Incident Handling Guide* describe the most commonly performed activities for attacking host identification:

    - **Validating the Attacking Host's IP Address:** New incident handlers often focus on the attacking host's IP address. The handler may attempt to validate that the address was not spoofed by verifying connectivity to it; however, this simply indicates that a host at that address does or does not respond to the requests. A failure to respond does not mean the address is not real, for example, a host may be configured to ignore pings and traceroutes. Also, the attacker may have received a dynamic address that has already been reassigned to someone else
    - **Researching the Attacking Host through Search Engines:** Performing an Internet search using the apparent source IP address of an attack may lead to more information on the attack, for example, a mailing list message regarding a similar attack
    - **Using Incident Databases:** Several groups collect and consolidate incident data from various organizations into incident databases. This information sharing may take place in many forms, such as trackers and real-time blacklists. The organization can also check its own knowledge base or issue tracking system for related activity
    - **Monitoring Possible Attacker Communication Channels:** Incident handlers can monitor communication channels that may be used by an attacking host. For example, many bots use IRC as the primary means of communication. Also, attackers may congregate on certain IRC channels to brag about compromises and share information. However, incident handlers should treat any such information acquired only as a potential lead, not as fact

- **Step 4:** Eradicate the incident and recover. Eliminate components of the incident (e.g. delete malware, disable breached accounts, identify and mitigate vulnerabilities that were exploited). Incident responders should coordinate with the IMT to identify and execute a strategy for eradication of the incident. Once eradication has been completed restore systems to normal operation, confirm that systems are functioning normally, and remediate vulnerabilities to prevent similar incidents

3.3.4 Post-Incident Activity

- **Step 1:** Conduct a lessons learned meeting. Learning and improving, one of the most important parts of incident response is also the most often omitted. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:
  - Exactly what happened, and at what times?
  - How well did staff and management perform in dealing with the incident? Were the documented procedures followed and adequate?
  - What information was needed sooner?
  - Were any steps or actions taken that might have inhibited the recovery?
  - What would the staff and management do differently the next time a similar incident occurs?
  - How could information sharing with other organizations have been improved?
  - What corrective actions can prevent similar incidents in the future?
  - What precursors or indicators should be watched for in the future to detect similar incidents?
  - What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

- **Step 2:** Document the lessons learned and update IRP and associated procedures as necessary

- **Step 3:** Ensure evidence is retained and archived. The criteria for evidence collection, a procedure to ensure a chain of custody, and archival instructions are maintained by the CCIC Forensic, Malware and Analysis Team (FMAT). The IMT will coordinate with the FMAT to provide incident responders with assistance to collect and handle evidence

3.3.5 Automated Incident Handling Processes (IR-04(01))

The purpose of this control is to ensure that CMS employs automated mechanisms to support the incident handling process. CMS employs automated mechanism (e.g., online incident management systems) to support the organization’s incident handling process. In the following table provides examples of tools used for automated incident handling processes at CMS.

Table 4: Automated Tools

Tools	Description	Users
RiskVision	Is the HHS tool used for all incident/tracking and reporting. Users do not access RiskVision directly	CMS IMT and IT Service Desk
CMS RSA Archer/CFACTS SecOps Module	It is used for tracking incident events, incidents events/response, and producing trends and metrics	CCIC IMT and CCIC SOC Analysts
Remedy	The CMS Remedy ticket is used by the CMS IT Service Desk to track changes and problems within the CMS environment	CMS IT Service Desk CCIC IMT and CCIC SOC Analysts CMS Users
Splunk	Is a logging solution for security (CMS Enterprise Security) and Operations and Maintenance (O&M) log management OCISO Systems Security Management (OSSM). It used as an audit reduction tool by the agency to review audit logs	CCIC

3.3.6 Continuity of Operations (IR-04(03))

The purpose of the Continuity of Operations control is to ensure that CMS identifies classes of incidents, defines actions to take in response to classes of incidents, and to ensure continuation of organizational missions and business functions specific process for Insider Threat-Specific Capabilities: The table below outlines the CMS organizationally defined parameters for IR Insider Threats – Continuity of Operations.

Table 5: CMS Defined Parameters - Control IR-4(03)

Control	Control Requirement	CMS Parameter
IR-4(03)	The organization identifies [Assignment: organization defined classes of incidents] and	Information systems owners and information security officers are responsible for aligning incident response plans and business continuity plans for the following classes of incidents:

Control	Control Requirement	CMS Parameter
	[Assignment: organization-defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions	o Malfunctions due to design/implementation errors and omissions o Targeted malicious attacks o Untargeted malicious attacks Information systems owners and information security officers are responsible taking one of the following actions in response to classes of incidents, as appropriate, and as directed by the IMT: o Graceful degradation o information system shutdown o Fall back to manual mode /alternative technology whereby the system operates differently o Employing deceptive measures o Alternate information flows, or o Operating in a mode that is reserved solely for when systems are under attack

Information Systems Owners and ISSOs are responsible for aligning incident response plans and business continuity plans for the following classes of incidents: malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Information Systems Owners and ISSOs are responsible for taking one of the following actions in response to classes of incidents, as appropriate. As directed by the IMT, the frontline incident responders should conduct a graceful degradation, information system shutdown, or fall back to manual mode/alternative technology. Additionally, when one of these actions is not feasible, additional actions might include employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.

3.3.7 Insider Threats-Intra-Organizations (IR-04(07))

The purpose of this control is to ensure that CMS coordinates incident-handling capability for insider threats. The table below outlines the CMS organizationally defined parameters for IR Insider Threats – Intra-Organization Coordination.

Table 6: CMS Defined Parameters - Control IR-04(07)

Control	Control Requirement	CMS Parameter
IR-4(07)	The organization coordinates an incident handling capability for insider threats across the organization [Assignment: organization-defined components or elements of the organization].	The IMT is responsible for coordinating incident handling on insider-threats with the CMS Counterintelligence and Insider Threat Program. The CMS Counterintelligence and Insider Threat Program will contact as needed across

Control	Control Requirement	CMS Parameter
		the organization, specifically with the following: ○ Mission/Business Owners ○ Information System Owners (ISO) ○ Office of Human Capital (OHC) ○ Office of Acquisitions and Grant Management (OAGM) ○ Personnel/Physical Security Offices (OSSO) ○ Operations Personnel ○ Cyber Risk Advisors (CRA)

Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example: Mission/Business Owners, ISOs, Office of Human Resources (OHR), Procurement Offices/Office of Acquisition and Grants Management (OAGM), Personnel/Physical Security Offices/ Office of Support Services and Operations, (OSSO), Operations Personnel, and Cyber Risk Advisors (CRA). The IMT is responsible for coordinating with the CMS Counterintelligence and Insider Threat Program on incident-handling capabilities for insider-threats across the organization.

3.3.8 Correlation with External Organizations (IR-04(08))

The purpose of the Correlation with External Organizations control is to ensure that CMS coordinates with both internal and external stakeholders to correlate and share incident information and to achieve a cross-organization perspective on incident awareness and more effective incident responses. For more information on internal threats procedures review Section 3.5 Incident Reporting. The table below outlines the CMS organizationally defined parameters for IR Correlation with External Organizations.

Table 7: CMS Defined Parameters - Control IR-4(08)

Control	Control Requirement	CMS Parameter
IR-4(08)	The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share. [Assignment: organization-defined incident information] to achieve a cross-organization perspective on	The IMT provides centralized coordination on incident awareness and incident response for all information systems across the CMS enterprise. The IMT will coordinate with the following external organizations: ○ Mission/business partners ○ Military/coalition partners ○ Customers, and ○ Multi-tiered developers The IMT will be responsible for sharing the following information with external parties:

	incident awareness and more effective incident responses.	o Description of the incident o Threat vectors o Steps taken to identify, eradicate, and recover from the incident

Correlation with external organizations is handled by the IMT. The IMT notifies external parties such as mission/business partners, military/coalition partners, customers, and multi-tiered developers as appropriate. The IMT will share incident information with appropriate external parties to achieve a cross-organization perspective on incident awareness and more affective incident response. Appropriate incident information includes the description of the incident, threat vectors, and steps taken to identify, eradicate, and recover from the incident. Additionally, appropriate incident information includes capability that allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization’s operations, assets, and individuals.

3.4 Incident Monitoring (IR-05)

The purpose of Incident Monitoring is to ensure that CMS documents information system security incidents and maintains records about each incident such as the status of the incident, and pertinent information necessary for forensics (evaluating incident details, trends, and handling). At CMS, the CCIC delivers a number of important, agency-wide security services. 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.[5]

The IMT is the group responsible for tracking and documenting security and privacy incidents. Stakeholders outside of the IMT (e.g., incident responders, ISSOs, system owners, etc.) are responsible for providing the information necessary to track and monitor information security and privacy incidents. Review Section 3.4 Incident Monitoring for details for tracking and monitoring information security incidents.

3.4.1 Automated Tracking/Data Collection/Analysis (IR-05(01))

The purpose of Automated Tracking/Data Collection/Analysis is to ensure that CMS employs automated mechanism to assist in the tracking of security incidents and in the collection and analysis of incident information. At CMS, the RSA Archer/CFACTS SecOps Module is utilized for tracking potential incidents under investigation by the CCIC SOC. The IMT is responsible for maintaining the data in RSA/CFACTS along with reviewing, updating, and analyzing the data and producing the trends analysis.

The following list details automated tools utilized at CMS to assist in the tracking of security incidents and in the collection and analysis of incident information. Once an incident has been reported, the external stakeholders will be able to leverage the benefits of these tools via the support provided by the IMT.

[5] For more detail see: *CMS Continuous Diagnostics and Mitigation Concept of Operations, Version .09, September 2015* (prepared by the CCIC)

- CMS uses a Remedy ticketing system for all privacy and security incidents for incident/tracking and reporting
- The CMS Remedy ticket is used by the CMS IT Service Desk to track changes and problems within the CMS environment
- The CMS Remedy ticket creates a shell ticket in RiskVision, which is the HHS incident response tool
- The CCIC IMT uses the information contained in the Remedy ticket to populate the ticket in RiskVision
- CMS RSA Archer/CFACTS SecOps Module is used for investigating potential incidents discovered by the CCIC SOC. If an potential incident is confirmed than the SOC Analyst opens up a ticket in RiskVision

3.5 Incident Reporting (IR-06)

The intent of this control is to ensure that CMS requires employees and contractors to report suspected information security and privacy incidents to appropriate authorities and to ensure that a formal incident reporting process exists.

As part of a robust, enterprise security operations program designed to reduce the risks of malicious activity, CMS established the CCIC to provide enterprise-wide situational awareness and near real-time risk management. The CCIC also provides information security and aggregated monitoring of security events across all CMS information systems. Finally, the CCIC notifies appropriate security operations staff of detected configuration weaknesses, vulnerabilities open to exploitation, relevant threat intelligence, including indicators of compromise (IOCs) and security patches. For purposes of incident response, the IMT as a sub-component of the CCIC provides incident response assistance and support. All information security and privacy incidents are to be reported to CMS IT Service Helpdesk. The CMS IT Service Helpdesk will notify the IMT as appropriate.

The table below outlines the CMS organizationally defined parameters for IR reporting.

Table 8: CMS Defined Parameters – Control IR-6

Control	Control Requirement	CMS Parameter
IR-6	a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]	a. One hour
	b. Reports security incident information to [Assignment: organization-defined authorities]	b. CMS IT Service Help Desk

The following process details the CMS procedure for reporting suspected security and privacy incidents:

- **Step 1:** Collect the supporting information on the suspected security and privacy incident using the Incident Response Reporting Template in Appendix K.

  Note: *This template replaces the previous HHS CMS Computer Security Incident Report form that was published separately to the information security library.*

- **Step 2:** Report the suspected information security and privacy incident to the CMS IT Service Desk at (410) 786-2580 (i.e., internal) or (800) 562-1963 (internal and external) and/or email CMS_IT_Service@cms.hhs.gov. All suspected information security and privacy incidents must be reported to the CMS IT Service Desk within an hour. DO NOT DELAY reporting of the incident
- **Step 3:** Provide the information contained on the completed incident reporting form to the CMS IT Service Desk
- **Step 4:** The CMS IT Service Desk creates a Remedy ticket and enters the details on the suspected security and privacy incident. This Remedy ticket creates a shell ticket in RiskVision, which is the HHS incident response tool
- **Step 5:** The IMT populates the RiskVision ticket using the details from the associated Remedy ticket
- **Step 6:** The IMT analyzes the suspected incident, working with the SOC analyst as necessary, and if confirmed as an actual incident executes the incident handling procedures located in Section 3.5 Incident Handling

3.5.1 Automated Reporting (IR-06(01))

The purpose of Automated Reporting is to ensure that CMS employs automated mechanisms to assist in the reporting of security and privacy incidents. The following steps detail the CMS specific process for Automated Reporting:

- **Step 1:** User will contact the CMS IT Service Helpdesk and report the security incident
- **Step 2:** The CMS IT Service Helpdesk will open a Remedy ticket and record the incident. This Remedy ticket creates a shell ticket in RiskVision, which is the HHS automated incident response tool
- **Step 3:** The CMS IT Service Helpdesk will assign a ticket to the IMT. The IMT populates the RiskVision ticket using the details from the associated Remedy ticket
- **Step 4:** The IMT will evaluate the event to see if the security incident is valid
- **Step 5:** If the IMT finds that the event is valid, the user will be contacted and the mitigation process will start
- **Step 6:** If the IMT finds that the event is not valid, the IMT will close out the ticket and contact the user

3.6 Incident Response Assistance (IR-07)

The purpose of Incident Response Assistance is to ensure that CMS provides an incident response support resource, integral to the CMS' incident capability that offers advice and assistance to users of the information system for handling and reporting of security and privacy incidents. The following steps detail the CMS specific process for Incident Response assistance:

- **Step 1:** User will contact the CMS IT Service Helpdesk for incident response assistance. The CMS IT Service Desk notifies the IMT as appropriate.
- **Step 2:** The IMT will evaluate and validate the incident and assist with the mitigation

3.6.1 Automation Support for Availability of Information/Support (IR-07(01))

The purpose of Automation Support for Availability of Information Support is to ensure that CMS employs automated mechanisms to increase the availability of incident response-related information and support.

CMS uses multiple resources to provide the user community information/support. These include but are not limited to intranets, mailboxes, and on-line libraries.

Users may use the following resources for Automation Support for Availability of Information/Support:

- The CMS website at https://www.cms.gov/
- The CMS CISO mailbox at CISO@cms.hhs.gov
- The CMS Intranet at http://Intranet.cms.gov (this service is available ONLY to personnel who have access to a GFE issued device, (i.e., laptop, desktop))
- The HHS.gov at https://www.hhs.gov
- The HHS Intranet at https://intranet.hhs.gov (this service is available ONLY to personnel who have access to a GFE issued device, (i.e., laptop, desktop))

3.6.2 Coordination with External Providers (IR-07(02))

The purpose of Coordination with External Providers is to ensure that CMS establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection, and identifies CMS incident response team members to the external providers.

CMS has established a cooperative relationship with its external providers such as contractors, US-CERT, local law/fire enforcement, the Internal Revenue Service (IRS), Health and Human Services (HHS) and other third parties.

The contact information for external providers are listed below but is not limited to this list:

- US-CERT, 245 Murray Lane SW, Arlington, VA, 20598-0645, (888)-282-0870
- Local law enforcement, Baltimore County Police Department, 6424 Windsor Mill Road, Windsor Mill, MD 21244, 410-887-1340
- Local fire enforcement, Baltimore County Fire Station 3, 7223 Windsor Mill Road, Baltimore, Maryland, MD 21244

- Internal Revenue Service, 1111 Constitution Ave NW, Washington, D.C., 20224, (202)-622-5000
- Health and Human Services, 200 Independence Avenue, S.W., Washington, D.C. 20201,1-877-696-6775

3.7 Incident Response Plan (IR-08)

The purpose of the Incident Response Plan (IRP) is to provide a roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements:

- Purpose
- Scope
- Definitions
- Roles and Responsibilities
- Understanding an Incident
- Incident Life Cycle
  - Preparation
  - Detection and Analysis
  - Containment, Eradication and Recovery
  - Post-Incident Activity
- Reporting Requirements
- Points of Contact

The incident response policy is established in the CMS IS2P2 and has been included in Section 1.5 Policy of this handbook. This document provides incident response procedure to facilitate the implementation of incident response controls. Incident response plan, policy, and procedure creation are an important part of establishing a team and permits incident response to be performed effectively, efficiently, and consistently; and so that the team is empowered to do what needs to be done.

The table below outlines the CMS organizationally defined parameters for IR planning.

Table 9: CMS Defined Parameters - Control IR-8

Control	Control Requirement	CMS Parameter
IR-8	a. Incident Response Plan is reviewed and approved by [Assignment: organization-defined personnel or role]; b. Distributes copies of the incident response plan to [Assignment organization-defined incident response personnel (identified by	a. Incident Response Plan is endorsed by CMS ISPG b. Copies of the Incident Response and Handling Plan has been distributed to all appropriate stakeholders to include: the CRA, ISSO,

Control	Control Requirement	CMS Parameter
	name and/or role) and organizational elements]	BO, Incident Responders, System Developers, and System Administrators
	c. Reviews the incident response plan [Assignment: organization-defined frequency];	c. Every 365 days
	d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;	d. Reviewed annually updated as required
	e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and Protects the incident response plan from unauthorized disclosure and modification	e. All stakeholders are informed of changes

The CCIC IMT created an IRP that provides the CMS with a roadmap for implementing its incident response capability and outlines the incident response process for the IMT. In addition, each information system is responsible for maintaining a separate IRP that describes the systems internal processes for incident response and leverages the capability of the IMT. The following steps details the process for creating an IRP using the template provided in Appendix L:

- **Step 1:** Complete a draft IRP by leveraging the template and instructions provided in Appendix L
- **Step 2:** Submit the draft IRP to the information system's assigned CRA for ISPG approval. Update that plan as necessary based on the feedback received from ISPG
- **Step 3:** Document the plan approval by having the Business Owner and ISSO sign the plan.
- **Step 4:** Disseminate the plan to all appropriate stakeholders to include: the CRA, ISSO, BO, Incident Responders, System Developers, and System Administrators

3.8 Information Spillage Response (IR-09)

The purpose of Information Spillage Response is to ensure that CMS responds to information spills.

As part of a robust, enterprise security operations program designed to reduce the risks of malicious activity, CMS established the CCIC to provide enterprise-wide situational awareness and near real-time risk management. The CCIC also provides information security and aggregated monitoring of security events, such as information spillage across all CMS information systems. For purposes of incident response and handling, the CCIC provides incident management services including corrective action direction and ensuring processes and procedures are followed as well as oversight to all CMS components. Reportable events and high impact incidents are to be reported to the CCIC via the Remedy ticket system. If access to Remedy is not directly available, this can be achieved by contacting the CMS IT Service Desk and requesting a security incident be opened. The table below outlines the CMS organizationally defined parameters for information spillage response.

Table 10: CMS Defined Parameters - Control IR-9

Control	Control Requirement	CMS Parameter
IR-9	b. Alerting [Assignment; organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill] f. Performing other [Assignment: organization-defined actions]	b. The IMT, by calling the CMS IT Service Desk f. Actions as directed by the IMT

The following process details the CMS procedure for information spillage response

- **Step 1:** Report the suspected spillage information to the CMS IT Service Desk at (410) 786-2580 (i.e., internal) or (1-800) 562-1963 (internal and external) and/or email CMS_IT_Service_Desk@cms.hhs.gov. All suspected spillage information must be reported to the CMS IT Service Desk within an hour. DO NOT DELAY reporting of the incident
- **Step 2:** Provide the information contained on the completed Incident Response Reporting Template to the CMS IT Service Desk. The template is found in Appendix K Incident Reporting Template
- **Step 3:** The CMS IT Service Desk creates a Remedy ticket and enters the details on the suspected spillage. This Remedy ticket creates a shell ticket in RiskVision, which is the HHS incident response tool
- **Step 4:** The IMT populates the RiskVision ticket using the details from the associated Remedy ticket
- **Step 5:** The IMT analyzes the suspected spillage, working with the SOC analyst as necessary, and if confirmed as an actual incident executes the incident handling procedures located in Section 3.5 Incident Handling

3.8.1 Information Spillage Response/Responsible Personnel (IR-09(01))

The purpose of Information Spillage Response/Responsible Personnel is to ensure that CMS assigns the appropriate personnel or roles with responsibility for responding to information spills. The IMT is the responsible personnel for responding to an information spillage and communicating with all necessary stakeholders to resolve the incident.

3.8.2 Information Spillage Response/Training (IR-09(02))

The purpose of Information Spillage Response Training is to ensure that CMS provides information response training to the personnel or roles within a specific timeframe. The table below outlines the CMS organizationally defined parameters for IR Information Spillage Response/Training.

Table 11: CMS Defined Parameters - IR-9(02)

Control	Control Requirement	CMS Parameter
IR-9(02)	a. The organization provides information spillage response training [Assignment: organization-defined frequency]	a. All users must take CMS Computer-based Training. Employees with specialized roles and responsibilities for security must take CMS Role-based Training

The following steps detail the CMS specific process for Information Spillage Response Training: For all EUA users the following steps outlined Computer-based Training (CBT), which includes the annual IR training.

- **Step 1:** The incident response training has been incorporated into the annual Security and Privacy Awareness Training therefore all EUA user must take the CBT Training located at https://www.cms.gov/cbt/forms/isspa.aspx. The training must be delivered to all EUA users initially prior to account issuance and annually thereafter
- **Step 2:** Each year based on the date of account issuance each user must receive an email requiring the review and completion of the annual CBT
- **Step 3:** Training records must be maintained using the CBT database and include the UID and the date the individual last completed the training
- **Step 4:** Media/Networking and Posting Organizational Information on Public Websites have been incorporated in the annual Security and Privacy Awareness Training and that the RoB is electronically signed as the last step of that training. Failing to complete the CBT training may result in the User having the credentials revoked

3.8.3 Post-Spill Operations (IR-09(03))

The purpose of Post Spill Operations is to ensure that CMS implements procedures to ensure information systems impacted by information spills can continue to carry out assigned tasks while performing corrective actions. The table below outlines the CMS organizationally defined parameters for post-spill operations.

Table 12: CMS Defined Parameters - IR-9(03)

Control	Control Requirement	CMS Parameter
IR-9(03)	The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	CMS monitors all VPN access for spillage, if a spillage is detected via malware or viruses, CMS will attempt to clean the device remotely. If this cannot be done, CMS will contact the user to bring the device for forensic analysis. A new device will be issued to the user while forensic analysis is completed.

The following steps detail the CMS specific process for Post-Spill Operations:

- **Step 1:** Contain the spillage, and identify all information hardware and software systems and applications affected, and take appropriate actions to ensure that the data spilled does not propagate further
- **Step 2:** Sanitize using approved utilities to permanently remove the data spilled from contaminated information systems, applications, and media
- **Step 3:** If sanitization is not affective, than applications and media needs to be replaced/reimaged

3.8.4 Exposure to Unauthorized Personnel (IR-09(04))

The purpose of Exposure to Unauthorized Personnel is to ensure that CMS employs a security and privacy safeguard for personnel having exposure to information not within assigned access authorizations. The table below outlines the CMS organizationally defined parameters for exposure to unauthorized personnel.

Table 13: CMS Defined Parameters - IR-9(04)

Control	Control Requirement	CMS Parameter
IR-9(04)	The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.	Makes personnel aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.

The following lists the security and privacy safeguards implemented by CMS for personnel exposed to information not within their assigned access authorizations:

- The individual's manager meets with the effected individual providing counsel and informing the individual of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.

3.9 Integrated Information Security Analysis Team (IR-10)

The purpose of the Integrated Information Security Analysis Team is to ensure that CMS establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

CMS established the CCIC to provide enterprise-wide situational awareness and near real-time risk management. The CCIC also provides information security and aggregated monitoring of security events across all CMS information systems. For purposes of incident response and handling, the CCIC provides incident management services including corrective action direction and ensuring processes and procedures are followed as well as oversight to all CMS components. Reportable events and high impact incidents are to be reported to the CCIC via the CMS Remedy ticket system. If access to Remedy is not directly available, this can be achieved by contacting the CMS IT Service Desk and requesting a security incident be opened.

Instances of loss, theft, or compromise of PII may involve an information security related malicious code attack or intrusion. In such cases, the Integrated Information Security Analysis Team are the organization's subject matter experts best able to support the organization's PII incident response team as required by OMB M-07-16. In addition to security implementers, developers, and operators; this internal team should also comprise of the Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy among others. The integrated information security analysis team will support the organization’s PII incident response team (as specified in OMB M-07-16) in all aspects of response to a security incident involving PII.

Appendix A. Acronyms

Selected acronyms used in this document are defined below.

Acronyms	Terms
AO	Authorization Official
ARS	Acceptable Risk Safeguards
BAT	Breach Analysis Team
CBT	Computer-based Training
CCIC	CMS Cybersecurity Integration Center
CDM	Continuous Diagnostics and Mitigation
CIA	Confidentiality, Integrity, Availability
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
CONOPS	Concept of Operations
CRA	Cyber Risk Advisor
CSIRC	Computer Security Incident Response Center
CSIRTs	Computer Security Incident Response Teams
DDoS	Distributed Denial of Service
DoS	Denial of Service
ERS	Enterprise Remedy System
EUA	Enterprise User Administration
FAQ	Frequently Asked Questions
FISMA 2014	Federal Information Security Modernization Act of 2014

Acronyms	Terms
FMAT	Forensics and Malware Analysis Team
FTI	Federal Tax Information
HHS	Health and Human Services
HHS CSIRC	HHS Computer Security Incident Response Center
HIPAA	Health Insurance Portability and Accountability Act of 1996
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IIR	Initial Incident Reporting
IMT	Incident Management Team
IOC	Indicators of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
IRA	Incident Response Authority
IRC	Internal Revenue Code
IRL	Incident Response Lead
IRC	Internal Revenue Code
IRP	Incident Response Plan
IRS	Internal Revenue Service
IRT	Incident Response Team
ISO	Information Systems Owners
ISP	Information Security Personnel
ISPG	Information Security and Privacy Group
ISSO	Information Systems Security Officer
IT	Information Technology

Acronyms	Terms
LAN	Local Area Network
LEOs	Law Enforcement Organizations
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVD	National Vulnerability Database
OCISO	Office of the Chief Information Security Officer
O&M	Operations and Maintenance
OMB	Office of Management and Budget
ODP	Organizational Defined Parameters
OPDIV	Operating Divisions
OS	Operating System
OSSM	OCISO Systems Security Management
OSSO	Office of Security and Support Operation
PCII	Protected Critical Infrastructure Information
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
POA&Ms	Plan of Action and Milestones
POC	Point of Contact
Pre-BAT	Pre-Breach Analysis Team
RMH	Risk Management Handbook
RV	RiskVision

Acronyms	Terms
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
SQL	Structured Query Language
SSN	Social Security Number
SSP	System Security Plan
SU	System User
SUID	Set User ID
TCP	Transmission Control Protocol
TIGTA	Treasury Inspector General for Tax Administration
TTL	Time to Live
UID	User ID
URL	Universal Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USGCB	U.S. Government Configuration Baselines
VPN	Virtual Private Network

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.
Administrative Vulnerability	An administrative vulnerability is a security weakness caused by incorrect or inadequate implementation of a system’s existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency. It is characterized by the fact that the full correction of the vulnerability is possible through a change in the implementation of the system or the establishment of a special administrative or security procedure for the system administrators and users. Poor passwords and inadequately maintained systems are the leading causes of this type of vulnerability.
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

Terms	Definitions
	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.
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
CMS Marketplace	The Affordable Care Act helps create a competitive private health insurance market through the creation of Health Insurance Marketplaces. These State-based, competitive marketplaces, which

Terms	Definitions
	launch in 2014, will provide millions of Americans and small businesses with "one-stop shopping" for affordable coverage.
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).
Data Compromise and Data Spills	Data compromise is the exposure of information to a person not authorized to access that information either through clearance level or formal authorization. This could happen when a person accesses a system he is not authorized to access or through a data spill. Data spill is the release of information to another system or person not authorized to access that information, even though the person is authorized to access the system on which the data was released. This can occur through the loss of control, improper storage, improper classification, or improper escorting of media, computer equipment (with memory), and computer generated output.
Data Destruction or Corruption	The loss of data integrity can take many forms including changing permissions on files so that files are writable by non-privileged users, deleting data files and or programs, changing audit files to cover-up an intrusion, changing configuration files that determine how and what data is stored and ingesting information from other sources that may be corrupt.
Denial of Service (DoS)	An action (or series of actions) that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, delay, or interruption of service. An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Enterprise User Administration	Manages the CMS user identifications. For more detail see https://portal.cms.gov/wps/portal/unauthportal/faq
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.

Terms	Definitions
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.
Exercise Briefing	Material that is presented to participants during an exercise to outline the exercise's agenda, objectives, scenario, and other relevant information.
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.
Full Live Test	Exercise plan incorporates real scenarios and injects into the exercise.
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.
Hotwash	A debrief conducted immediately after an exercise or test with the staff and participants.

Terms	Definitions
Hybrid Test	An exercise with some live scenarios facilitated by a response team for realism (probes, scans, email spoofing, etc.);
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.

Terms	Definitions
Information Technology	The term information technology with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment that is 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. 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.
Injects	Injects are scenario based exercises created by a functional exercise team during one of several phases (e.g., Development Phase, Conduct Phase for testing, training and exercise programs for IT plans and capabilities). An example inject is: A Controller would play the role of the Chief Information Officer and would call the Team Chief to provide information and request follow-on action. Expected actions by the Team chief or other exercise participants are documented, to aid controllers, simulators, or data collectors in anticipating what actions will result from the inject. For more information on injects see: NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (page B-8 at: http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
Insider Attack	Insider attacks can provide the greatest risk. In an insider attack, a trusted user or operator attempts to damage the system or compromise the information it contains
Insider Threat	An insider threat is 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 and

Terms	Definitions
	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.
Intrusions or Break-Ins	An intrusion or break-in is entry into and use of a system by an unauthorized individual.
Malicious Code	Malicious code is software or firmware intentionally inserted into an information system for an unauthorized purpose.
Malicious Software (Malware)	Malicious code is software based attacks used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem. The following is a brief listing of various software attacks: 1. **Virus:** It is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data). 2. **Worm:** An unwanted, self-replicating autonomous process (or set of processes) that penetrates computers using automated hacking techniques. 3. **Trojan Horse:** A useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data. 4. **Spyware:** Surreptitiously installed malicious software that is intended to track and report the usage of a target system or collect other data the author wishes to obtain. 5. **Rootkit Software:** Software intended to take full or partial control of a system at the lowest levels. Contamination is defined as inappropriate introduction of data into a system. 6. **Privileged User Misuse:** Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains. 7. **Security Support Structure Configuration Modification:** Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled, being an essential to maintaining the security policies of the system

Terms	Definitions
	Unauthorized modifications to these configurations can increase the risk to the system.
Master Scenario Events List (MSEL)	A chronologically sequence outline of the simulated events and key event descriptions that participants will be asked to respond to during an exercise.
Message Inject	A pre-scripted message that will be given to participants during the course of an exercise.
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.
Paper Inject/Event	A specific activity executed as part of a Master Scenarios Event List (MSEL), MSEL is a collection of pre-scripted events intended to guide an exercise towards specific outcomes. Paper injects drive exercise play. The exercise planning process determines the participants, exercise scenario, injects and the execution order of the course of the exercise. Planners must tailor injects for each exercise to meet the desired outcomes. For example, if the exercise centers on assessing the ability to detect and properly react to hostile activity, the exercise planners would need to structure one or more scenarios that involve hostile activities against the target IT assets. The exercise planner would design these scenarios to stimulate the training audience and elicit responses that that match the desired outcomes of the specific exercise and the overarching objectives.
Participant Guide	An exercise document that typically contains the exercise's purpose, scope, objectives, and scenario, and a copy of the IT plan being exercised.
Planner(s)	The group responsible for planning and executing the exercise in a realistic manager.
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,

Terms	Definitions
	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. 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.

Terms	Definitions
Pre-Breach Analysis Team	The CMS Pre-BAT, managed by the CMS Information Security and Privacy Group, with the assistance from the CMS Business Owner/Information Systems Owner (ISOs) and SOP staff as necessary, reviews, triages privacy incidents, and refers to the CMS BAT for a formal risk assessment when needed.
Privileged User Misuse	Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains.
Red Team	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.
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.
RiskVision	Incident report and tracking system used by HHS and CMS.
Rootkit Software	A type of malicious software (Malware) - Software that is intended to take full or partial control of a system at the lowest levels. Contamination is defined as inappropriate introduction of data into a system.
RSA Archer	RSA Archer is a modulated platform that assists in building an efficient, collaborative governance, risk and compliance (GRC) program. For more details see: http://www.ndm.net/rsa/Archer-GRC/archer-grc-modules
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

Terms	Definitions
	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 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.
Spillage	Instances where sensitive information (e.g. classified information, export-controlled information) is inadvertently place on information systems that are not authorized to process such information.
Spyware	A type of malicious software (Malware) that is surreptitiously installed and intended to track and report the usage of a target system or collect other data the author wishes to obtain.
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing the roles during an emergency and the responses to particular emergency. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
Tabletop Test	An exercise with injects scripted by exercise planners and delivered via paper (cards/discussion).

Terms	Definitions
Technical Vulnerability	A technical vulnerability is a hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally, thus increasing the risk of compromise, alteration of information, or denial of service.
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 that will be performed for a particular test, including the required logistical items and expected outcome or response for each step.
Test, Training, and Exercise (TT&E) Event	An event used to support the maintenance of an IT plan by allowing organizations to identify problems related to an IT plan and implement solutions before an adverse situation occurs.
Test, Training, and Exercise (TT&E) Plan	A plan that outlines the steps to be taken to ensure that personnel are trained in IT plan roles and responsibilities. TT&E plans are exercised to validate the viability of how IT components or systems are tested and to validate the operability in the context of an IT plan.
Test, Training, and Exercise (TT&E) Policy	A policy that outlines an organization's internal and external requirements associated with training personnel, exercising IT plans, and testing IT components.
Test, Training, and Exercise (TT&E) Program	A means for ensuring that personnel are trained in IT plan roles and responsibilities; TT&E plans are exercised to validate the viability; and how IT components or systems are tested to validate operability.
Test, Training, and Exercise (TT&E) Program Coordinator	A person who is responsible for developing a TT&E plan and coordinating TT&E events.
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.
Trojan Horse	A type of malicious software (Malware) – a useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data.

Terms	Definitions
Virus	A type of malicious software (Malware) that is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data).
Vulnerabilities	Any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.
Worm	A type of malicious software (Malware) that is an unwanted, self-replicating autonomous process (or set of processes that penetrates computers using automated hacking techniques.

Appendix C. Applicable Laws and Guidance

Appendix C provides references to both authoritative and guidance documentation supporting the "document." Subsections are organized to "level of authority" (e.g., Statues take precedence over Federal Directives and Policies). The number on each reference represents a mapping which uniquely identifies the reference within the main body of the document. 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 GAO-14-354, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*

http://www.gao.gov/assets/670/662901.pdf

3 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

http://www.hhs.gov/hipaa/

4 IRS Publication 1075 (October 2014)

https://www.irs.gov/pub/irs-pdf/p1075.pdf

5 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

6 US-CERT Federal Incident Notification Guidelines

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

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 Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB Memorandum M-03-22)

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

3 OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

4 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

5 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

6 OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.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 800-40 r3, *Creating a Patch and Vulnerability Management Program*

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

5 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

6 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

7 NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide, dated March 2008*

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

8 NIST SP 800-70 r3 *National Checklist Program for IT Products — Guidelines for Check list Users and Developers*

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r3.pdf

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

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

10 US-CERT Federal Incident Notification Guidelines

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

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

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

C.5 HHS Policy

1 *HHS-OCIO-2013-0004 HHS Policy for Personal Use of Information Technology Resources*

http://www.hhs.gov/ocio/policy/pol-pers-use-it-resources.html (Intranet Only)

2 *HHS-OCIO-2014-0001 HHS Information System Security and Privacy Policy (HHS IS2P)*

HHS Information Security and Privacy Policy (IS2P) – 2014 Edition. 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 The Office of the Assistant Secretary for Financial Resources (ASFR)*

http://www.hhs.gov/about/agencies/asfr/ (Intranet Only)

5 *HHS Office of Grants and Acquisition Policy and Accountability (OGAPA)*

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

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

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

7 *HHS-CSIRT Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response*

http://www.hhs.gov/ocio/policy/hhs_ocio_policy_2010_0004.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

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

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

C.7 Associated CMS Resources

1 HHS Departmental Security Policy and Standard Waiver Form

http://intranet.hhs.gov/it/cybersecurity/policies/index.html (Accessible via intranet only)

2 CMS Policy for Acceptable Use of CMS Desktop/Laptop and Other IT Resources

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/Policy-CMS-Policy-for-the-Acceptable-Use-of-CMS-Desktop-Laptop-and-Other-IT-Resources.html

3 Risk Management Handbook Volume II Procedure 3.3-Common Control Identification

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VII_3-3_Common_Control_Identification.pdf

4 CMS Technical Reference Architecture 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

5 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

6 Technical Review Board Charter Version: 3.0 Last Modified: September 5, 2014

http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/TRBCharter.pdf

7 Risk Management Handbook Volume I Chapter 1 – Risk Management in the XLC Version 1.0 November 8,

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Vol-I-Chapter-01-Risk-Management-in-the-XLC.html?DLPage=1&DLEntries=10&DLFilter=XLC&DLSort=0&DLSortDir=ascending

Appendix D. ARS Standards – Incident Response (IR)

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
IR-01	High, Moderate, Low the	Incident Response Policy and Procedures	a. Develops, documents, and disseminates to applicable personnel: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls. b. Reviews and updates (as necessary) the current: 1. Incident response policy within every three (3) years; and 2. Incident response procedures within every three (3) years.	Applicable personnel (item a) include the Incident Response Team as required by OMB M-07-16	
IR-02	High, Moderate, Low	Incident Response Training	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within one (1) month of assuming an incident response role or responsibility; b. b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter. IMPLEMENTATION STANDARD(S) Std.1 - Formally tracks personnel participating in incident response training.		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
IR-02(01)	High Moderate	Simulated Events	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. IMPLEMENTATION STANDRD: Std.1 - Formally tracks personnel participating in incident response training.		
IR-03	High, Moderate	Incident Response Testing	The organization tests the incident response capability for the information system within every three hundred sixty-five (365) days using NIST SP 800-61, reviews, analyses, and simulations to determine the incident response effectiveness and documents. IMPLEMENTATION STANDARDS: Std.1 - Incident response capability tests must exercise (or simulate exercise of) all organizational response capabilities. The organization's documented response to an actual historic incident may be used as part of an incident response capability test, and any response capabilities that were not exercised as part of the historic incident response must be additionally exercised (or simulated) as part of the test.		
IR-03(01)	High	Automated Testing	The organization: a. Tests incident response capability using: 1. Checklists; 2. Walk-through, discussion-based, or tabletop exercises; 3. Comprehensive, functional exercises executed in a simulated operational environment; and 4. Automated mechanisms, as applicable.		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			b. Documents results for assessment and potential process improvement. IMPLEMENTATION STANDARDS: Std. 1 - An exercise is a scenario-driven simulation of a situation designed to validate the viability of one or more aspects of an IT plan. Std. 2 - Functional exercises vary in complexity and scope from specific aspects to full-scale scenarios that address all plan elements. Std. 3 - Organizations should conduct tests of IR capability periodically, especially following organizational changes, updates to an IT plan, issuance of new IR guidance or as needed.		
IR-03(02)	High, Moderate	Coordination with Related Plans	The organization coordinates incident response testing with organizational elements responsible for related plans.		
IR-04	High, Moderate, Low	Incident Handling	The organization: a. Implements an incident handling capability (i.e., system incident response plan) using the current RMH Chapter 8 Incident Response; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly. IMPLEMENTATION STANDARDS: Std.1 - Document relevant information related to a security incident according to the current		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			CMS Incident Handling and Breach Notification Standard and Procedures. Std.2 - Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence (i.e., Federal Rules of Evidence). Std.3 - Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolation or system disconnect. Std.4 - Incident response activities, to include forensic malware analysis, is coordinated with the Information System Security Officer (ISSO) and the CMS Cybersecurity Integration Center (CCIC). Each organization's security operations center: a. Is responsible for actions to reduce the risk that an information security and/or privacy incident will occur and to respond appropriately to each incident or breach; and b. Maintains primary responsibility for incident detection, including internal security monitoring and analysis of network traffic and logs. Std.5 - Contact information for individuals with incident handling responsibilities must be maintained within CFACTS. a. Changes must be documented within CFACTS within three (3) days of the change.		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
IR-04(01)	High, Moderate	Automated Incident Handling Processes	The organization employs automated mechanisms to support the incident handling process. IMPLEMENTATION STANDARDS: Std.1 - Automated mechanisms support the exchange of incident handling information with the CMS Cybersecurity Integration Center (CCIC): a. Information is provided to the CCIC in a format compliant with CMS and federal requirements; b. Incident handling information sources include systems, appliances, devices, services, and applications (including databases); c. Incident handling information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and d. CCIC directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.		
IR-04(03)	High, Moderate	Continuity of Operations	The organization identifies incidents and responses to classes of incident to ensure continuation of organizational missions and business functions. Classes of incident are based on attack vector (e.g., attack via external media, the web, improper system	(For PHI Only) The organization identifies emergencies, vandalism, security incidents, or natural disasters and reasonable and	

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			use, and loss of equipment) and serve to further define specific handling procedures. IMPLEMENTATION STANDARDS: Std.1 - Incident response policies/procedures and business continuity processes should be aligned. Computer security incidents undermine the business resilience of an organization. Business continuity planners should be made aware of incidents, the impacts, and steps to adjust business impact, risk, and continuity of operations assessments and plans. Std.2 - Organizations should create written guidelines for prioritizing incidents.	appropriate policies and procedures consistent with federal laws and regulations and organizational requirements to ensure continuation of organizational missions and business functions.	
IR-04(04)	High	Information Correlation	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.		
IR-04(06)	High, Moderate, Low	Insider Threats – Specific Capabilities	The organization defines and implements the incident handling capability for insider threats. IMPLEMENTATION STANDARDS: Std.1 - In accordance with HHS policy, the CMS CIO must carry out monitoring in a manner that protects employee interests and ensures the need for monitoring has been thoroughly vetted and documented. Std.2 - All requests from outside law enforcement agencies must be coordinated through the HHS Office of Inspector General (OIG), except for requests relating to national security or non-criminal insider threat matters, which must be coordinated with the HHS Office of Security and Strategic Information (OSSI) and/or the CMS Security Management		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			Group, Division of Physical Security and Strategic Information. Std.3 - No CMS official may initiate computer monitoring without advance written authorization by the CMS Administrator or the CMS CIO. Std.4 - Computer monitoring may only be authorized for the following reasons: a. Monitoring has been requested by the HHS OSSI, the HHS OIG, or an outside law enforcement authority in accordance with CMS Security Management Group, Division of Physical Security and Strategic Information, and federally recognized jurisdiction; b. Reasonable grounds exist to conclude that the individual to be monitored may be responsible for an unauthorized disclosure of legally protected information (e.g., confidential commercial information or Privacy Act protected information); and c. Reasonable grounds exist to believe that the individual to be monitored may have violated an applicable law, regulation, or written HHS or CMS policy. Std.5 - In circumstances in which HHS OIG requests computer monitoring for purposes of an HHS OIG investigation or where HHS OIG requires assistance in the conduct of computer monitoring, HHS OIG will provide such information or notification as is consistent with its responsibilities, duties, and obligations under the Inspector General Act of 1978. a. In concert with the HHS Office of General Counsel (OGC), the CMS CIO must		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			develop a memorandum of understanding (MOU) or similar written agreement with outside law enforcement agencies as a precondition for approving monitoring requests from these organizations. The MOU must include the following: • Title and organizational component of the person(s) authorized to make monitoring requests on behalf of the law enforcement agency; • Documentation of the source of the official request, demonstrating approval by an official of the governmental entity that has the authority to request the initiation of such monitoring (e.g., a subpoena [administrative or grand jury], warrant, national security letter [NSL], or other acceptable documented request [e.g., a written law enforcement administrative request that meets applicable requirements of the Privacy Act and/or HIPAA requirements for certain disclosures to law enforcement agencies]); • Any restrictions applicable to the handling and disclosure of confidential information that may be produced by monitoring; • Other items consistent with this memorandum, including handling sensitive communications, as described in the following bullet, Documentation; • Documentation – the written authorization for computer monitoring		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			describes the reason for the monitoring. If the monitoring is initiated at the request of outside law enforcement authorities, the authorization documents that the request was approved, consistent with the applicable MOU with that organization by an official of the governmental entity that has the authority to request the initiation of such monitoring. b. Except for monitoring initiated at the request of an outside law enforcement authority or the HHS OIG, the party requesting the monitoring must document the factual basis justifying the request for monitoring and the proposed scope of the request. Requests for such monitoring must include an explanation of how monitoring will be conducted, how the information collected during monitoring will be controlled and protected, and a listing of individuals who will have access to the resulting monitoring information. c. A record of all requests for monitoring must be maintained by the CMS CIO, along with any other summary results or documentation produced during the period of monitoring. The record must also reflect the scope of the monitoring by documenting search terms and techniques. All information collected from monitoring must be controlled and protected, with distribution limited to the individuals identified in the request for monitoring and other individuals		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			specifically designated by the CMS Administrator or CMS CIO as having a specific need to know such information. Std.6 - The CMS Administrator or CMS CIO must ensure authorized computer monitoring is appropriately narrow in scope and time limited and takes the least invasive approach to accomplish monitoring objectives. The CMS Administrator or CMS CIO, in reviewing requests for monitoring, must consider whether there are alternative information gathering methods that CMS can utilize to address the concern in lieu of monitoring. When the monitoring request originates from HHS OIG or outside law enforcement, CMS will grant appropriate deference to a request made in accordance with this policy. Std.7 - No monitoring authorized or conducted may target communications with law enforcement entities, the Office of Special Counsel, members of Congress or staff, employee union officials, or private attorneys. Employee union officials of CMS will be treated, for non-targeted monitoring purposes, as all other employees of CMS, when monitoring is necessary. If such protected communications are inadvertently collected or identified from more general searches, the communications may not be shared with a non-law enforcement party who requested the monitoring or anyone else without express written authorization from the HHS OGC and other appropriate HHS official(s). Std.8 - When a request for computer monitoring is made by a party other than an outside law enforcement authority or the HHS		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			OIG, CMS must consult with the OGC as to whether the monitoring is consistent with all applicable legal requirements, including the Whistleblower Protection Act and HIPAA, and consider whether there are any additional limits. In addition, except for monitoring initiated at the request of outside law enforcement or the HHS OIG, parties that receive information derived from monitoring must consult with the OGC as to potential restrictions on the use of such information under applicable law. Std.9 - The CMS CIO must review all employee monitoring on a monthly basis and, in consultation with the party who requested the monitoring, assess whether it remains justified or is to be discontinued. The CMS CIO must consider if the decision for ongoing monitoring must be reviewed by the OGC. A decision to continue monitoring must be explained and documented in writing by the CMS CIO, who must report no less often than monthly to the CMS Administrator regarding the status of any ongoing monitoring. Std.10 - The CMS CIO and the OGC may make recommendations to the CMS Administrator for additional procedures, if necessary, to address specific circumstances not addressed in this policy. Insider threat policies and procedures that deviate from the elements of this policy, however, must not be implemented without the written concurrence of the HHS CIO in consultation with the OGC.		
IR-04(07)	High, Moderate, Low	Insider Threats – Intra-Organization Coordination	The organization coordinates with the CMS Counterintelligence and Insider Threat		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			Program on incident handling capability for insider threats across the CMS enterprise. IMPLEMENTATION STANDARDS: Std.1 - Insider threat coordination must be in accordance with the insider threat capability defined by CMS.		
IR-04(08)	High, Moderate, Low	Correlation with External Organizations	CMS coordinates and shares threat and incident information with Federal and industry cybersecurity organizations to achieve a cross organization perspective on incident awareness and more effective incident responses. IMPLEMENTATION STANDARDS: Std.1 - The CMS Cybersecurity Integration Center (CCIC) provides centralized coordination on incident awareness and incident response for all information systems across the CMS enterprise. Std.2 - The CCIC provides centralized coordination and sharing on incident awareness and incident response with external organizations.		IR-04(08)
IR-05	High, Moderate, Low	Incident Monitoring	The organization tracks and documents all physical, information security, and privacy incidents. IMPLEMENTATION STANDARDS: Std.1 - The organization forwards information security and privacy incident and breach information: • In accordance with reporting requirements defined under the current RMH Chapter 8 Incident Response		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			• - Provides incident and breach information in format compliant with CMS and federal (e.g., Continuous Diagnostics and Mitigation [CDM]) requirements.		
IR-05(01)	High	Automated Tracking/Data Collection/Analysis	The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.		
IR-06	High, Moderate, Low	Incident Reporting	The organization: a. Requires personnel to report actual or suspected security and privacy incidents to the organizational incident response capability within the timeframe established in the current RMH Chapter 8 Incident Response; and b. Reports security incident information to authorities (defined in the system security plan [SSP]) and in Implementation Standard 1. IMPLEMENTATION STANDARDS: Std.1 - Designated authorities must include the CMS Cybersecurity Integration Center (CCIC). The CCIC provides oversight of information security and privacy, to include incident reporting, for each FISMA System operating by or on behalf of CMS.		
IR-06(01)	High, Moderate	Automated Reporting	The organization employs automated mechanisms to assist in the reporting of security incidents.		
IR-06(02)	High, Moderate, Low	Vulnerabilities Related to Incidents	CMS coordinates and shares threat and incident information with federal and industry cybersecurity organizations to achieve a cross organization perspective on incident		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			awareness and more effective incident responses. IMPLEMENTATION STANDARDS: Std.1 - The CMS Cybersecurity Integration Center (CCIC) provides centralized coordination on incident awareness and incident response for all information systems across the CMS enterprise. Std.2 - The CCIC provides centralized coordination and sharing on incident awareness and incident response with external organizations		
IR-07	High, Moderate, Low	Incident Response Assistance	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. IMPLEMENTATION STANDARDS: Std.1 - The CCIC provides centralized coordination and assistance on information security and privacy incident/breach awareness and management for all information systems across the CMS enterprise.		
IR-07(01)	High, Moderate	Automation Support for Availability of Information/Support	The organization employs automated mechanisms to increase the availability of incident response-related information and support.		
IR-07(02)	High, Moderate, Low	Coordination with External Providers	The organization: a. Establishes a direct, cooperative relationship between its incident response capability and external providers of		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			information system protection capability; and b. Identifies organizational incident response team members to the external providers.		
IR-08	High, Moderate, Low	Incident Response Plan	The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by the applicable Incident Response Team Leader; b. Distributes copies of the incident response plan to: • CMS Chief Information Security Officer; • CMS Chief Information Officer; • Information System Security Officer;		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			- CMS Office of the Inspector General/Computer Crimes Unit; - All personnel within the organization Incident Response Team; - All personnel within the PII Breach Response Team; and - All personnel within the organization Operations Centers. c. Reviews the incident response plan within every three hundred sixty-five (365) days; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to the organizational elements listed in b. above; and f. Protects the incident response plan from unauthorized disclosure and modification.		
IR-09	High	Information Spillage Response	The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting incident response personnel (as defined in the SSP and the incident response plan [See IR-6]) of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component;		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing required response actions as in the system incident response plan.		
IR-09(01)	High, Moderate	Responsible Personnel	The organization assigns responsibility for responding to information spills to defined personnel or roles. IMPLEMENTATION STANDARDS: Std.1 - Contact information for individuals with responsibility for responding to information spills must be maintained within CFACTS. a. Changes must be documented within CFACTS within seven (7) days of the change.		
IR-09(02)	High, Moderate	Training	The organization provides information spillage response training no less often than annually.		
IR-09(03)	High, Moderate	Post-Spill Operations	The organization implements processes procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.		
IR-09(04)	High, Moderate	Exposure to Unauthorized Personnel	The organization employs CMS rules of behavior and information system defined security safeguards and privacy to address the risk of personnel exposed to information not within assigned access authorizations.		
IR-10	High, Moderate, Low	Integrated Information Security Analysis Team	The organization implements processes procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.		

Control Number	Baseline	Control Name	CMS Control	Privacy Controls	CSP/FedRAMP Control
			IMPLEMENTATION STANDARDS: Std.1 - The CMS Cybersecurity Integration Center (CCIC) provides oversight and coordination of information security and privacy incident response teams, to include forensic malware analysis, for each FISMA System operating by or on behalf of CMS. Std.2 - The organization must integrate information security capabilities and services with the CCIC, including coordination among the CMS CISO, business owners, Information System Security Officers (ISSO), and other stakeholders within the timeframes required by CMS or other federal mandate. Std.3 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational security status and posture information.		

Appendix E. Control/Policy Cross Reference Table

NIST SP 800-53r4 IR Control	CMS ARS IR Control	CMS IS2P2 Policy	HHS IS2P Policy
IR-1 Incident Response Policy and Procedures	IR-01 Incident Response Policy and Procedures	IR-1, IR-1.1.1, IR-1.1.14, IR-1.1.43, IR-1/1/5	IR-1 Incident Response Policy and Procedures
IR-2 Incident Response Training	IR-02 Incident Response Training	IR-1.1.43, IR-1.1.5	IR-2 Incident Response Training
IR-2(1) Incident Response Training | Simulated Events	IR-02(01) Simulated Events	IR-1.1.43, IR-1.1.5	IR-2 c.e1 Simulated Events
IR-2(2) Incident Response Training | Automated Training Environments	IR-02(02) Automated Training Environments	IR-1.1.43, IR-1.1.5	IR-2 c.e.2 Automated Training Environments
IR-3 Incident Response Testing	IR-03 Incident Response Testing	IR-1.1.4.2, IR-1.1.4.3	IR-3 Incident Response Testing
IR-3(1) Incident Response Testing | Automated Testing	IR-03(01) Automated Testing	IR-1.1.4.2, IR-1.1.4.3	IR-3 c.e.1 Automated Testing
IR-3(2) Incident Response Testing | Coordination with Related Plans	IR-03(02) Coordination with Related Plans	IR-1.1.4.2, IR-1.1.4.3	IR-3 c.e.2 Coordination with Related Plans
IR-04 Incident Handling	IR-04 Incident Handling	IR-1, IR-1.1.1, IR-1.1.4.3, IR-1.2.1	IR-4 Incident Handling
IR-4(1) Incident Handling | Automated Incident Handling Processes	IR-04(01) Automated Incident Handling Processes	IR-1, IR-1.1.1,IR-1.1.4.3, IR-1.2.1	IR-4 c.e.1 Automated Incident Handling Processes
IR-4(3) Incident Handling | Continuity of Operations	IR-04(03) Continuity of Operations	IR-1, IR-1.1.1,IR-1.1.4.3, IR-1.2.1	IR-4 c.e.3 Continuity of Operations
IR-4(4) Incident Handling | Information Correlation	IR-04(04) Information Correlation	IR-1, IR-1.1.1,IR-1.1.4.3, IR-1.2.1	IR-4 c.e.4 Information Correlation

NIST SP 800-53r4 IR Control	CMS ARS IR Control	CMS IS2P2 Policy	HHS IS2P Policy
IR-4(6) Incident Handling | Insider Threats – Specific Capabilities	IR-04(06) Insider Threats Specific Capabilities	IR-1, IR-1.1.1,IR-1.1.4.3, IR-1.2.1	IR-4 c.e.6 Insider Threats-Specific Capabilities
IR-4(7) Incident Handling | Insider Threats – Intra-Organization Coordination	IR-04(07) Insider Threats – Intra-Organization Coordination	IR-1, IR-1.1.1,IR-1.1.4.3, IR-1.2.1	IR-4 c.e.7 Insider Threats-Intra-Organization Coordination
IR-4(8) Incident Handling | Correlation with External Organizations	IR-04(08) Correlation with External Organizations	IR-1, IR-1.1.1,IR-1.1.4.3, IR-1.2.1	IR-4 c.e.8 Correlation with External Organizations
IR-05 Incident Monitoring	IR-05 Incident Monitoring	IR-1	IR-5 Incident Monitoring
IR-5(1) Incident Monitoring | Automated Tracking/Data Collection/Analysis	IR-05(01) Automated Tracking/Data Collection/Analysis	IR-1.3	IR-5 c.e.1 Automated Tracking/Data Collection/Analysis
IR-6 Incident Reporting	IR-06 Incident Reporting	IR-1.1.1	IR-6 Incident Reporting
IR-6(1) Incident Reporting | Automated Reporting	IR-06(01) Automated Reporting	IR-1.1.1	IR-6 c.e.1 Automated Reporting
IR-6(2) Incident Reporting | Vulnerabilities Related to Incidents	IR-06(02) Vulnerabilities Related to Incidents	IR-1	IR-6 c.e.2 Vulnerabilities Related to Incidents
IR-07 Incident Response Assistance	IR-07 Incident Response Assistance	IR-1	IR-7 Incident Response Assistance
IR-7(1) Incident Response Assistance | Automation Support for Availability of Information /Support	IR-07(01) Automation Support for Availability of Information/Support	IR-1	IR-7 c.e.1 Automation Support for Availability of Information/Support
IR-7(2) Incident Response Assistance | Coordination with External Providers	IR-07(02) Coordination with External Providers	IR-1	IR-7 c.e.2 Coordination with External Providers
IR-8 Incident Response Plan	IR-08 Incident Response Plan	IR-1	IR-8 Incident Response Plan

NIST SP 800-53r4 IR Control	CMS ARS IR Control	CMS IS2P2 Policy	HHS IS2P Policy
IR-9 Information Spillage Response	IR-09 Information Spillage Response	IR-1.1.3, IR-1.1.4, IR-1.1.4.1, IR-1.1.4.2, IR-1.1.4.3, IR-1.1.5, IR-1.2	IR-9 Inform Spillage Response
IR-9(1) Information Spillage Response | Responsible Personnel	IR-09(01) Responsible Personnel	IR-1.1.3	IR-9 c.e.1 Responsible Personnel
IR-9(2) Information Spillage Response | Training	IR-09(02) Training	IR-1.1.4.3, IR-1.1.5	IR-9 c.e.2 Training
IR-9(3) Information Spillage Response | Post Spill Operations	IR-09(03) Post-Spill Operations	IR-1	IR-9 c.e.3 Post Spill Operations
IR-9(4) Information Spillage Response | Exposure to Unauthorized Personnel	IR-09(04) Exposure to Unauthorized Personnel	IR-1	IR-9 c.e.4 Exposure to Unauthorized Personnel
IR-10 Integrated Information Security Analysis Team	IR-10 Integrated Information Security Analysis Team	IR-1	IR-10 Integrated Information Security Analysis Team

Appendix F. Impact Classifications & Threat Vectors Descriptions

Impact Classifications	Impact Description
Functional Impact	**HIGH** – Organization has lost the ability to provide all critical services to all system users. **MEDIUM** – Organization has lost the ability to provide a critical service to a subset of system users. **LOW** – Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance. **NONE** – Organization has experienced no loss in ability to provide all services to all users.
Information Impact	**CLASSIFIED** – The confidentiality of classified information was compromised. **PROPRIETARY**– The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised. **PRIVACY** – The confidentiality of personally identifiable information 7 (PII) or personal health information (PHI) was compromised. **INTEGRITY** – The necessary integrity of information was modified without authorization. **NONE** – No information was exfiltrated, modified, deleted, or otherwise compromised.
Recoverability	**REGULAR** – Time to recovery is predictable with existing resources. **SUPPLEMENTED** – Time to recovery is predictable with additional resources. **EXTENDED** – Time to recovery is unpredictable; additional resources and outside help are needed. **NOT RECOVERABLE** – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly). **NOT APPLICABLE** – Incident does not require recovery.

Threat Vectors	Description	Example
Unknown	Cause of attack is unidentified	This option is acceptable if cause (vector) is unknown upon initial report. The threat vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures

Threat Vectors	Description	Example
Web	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	Spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack does not fit into any other vector	

Appendix G. Tabletop Exercise Test Plan Template

Test Topic	*<Insert Topic>*
Test Scope	*<Describe the scope of the incident response test to include who will participate in the exercise, the purpose of the test, and the expected outcome. All personnel with responsibilities under the incident response plan should participate in the exercise. The exercise should apply to the roles and responsibilities. This includes personnel within the incident response plan being exercised and focus on validating that the documented roles, responsibilities, and interdependencies are accurate and current. To ensure that the knowledge of the roles and responsibilities identified in the plan being exercised is current, it is often effective to conduct a training session in conjunction with any tabletop exercise.>*
Test Objectives	The objectives of this test is as follows:
1	To validate the content of the incident response plan and the related policies and procedures.
2	Validate participants' roles and responsibilities as documented in the incident response plan and validate the interdependencies documented in the incident response plan.
3	To meet regulatory requirements specifically the NIST SP 800-53 Rev. 4 requirements for incident response testing and incident response training.
4	To document lessons learned that may be utilized to update the incident response plan and related policies and procedures.
Participants	*<Insert participants, the participants should be comprised of personnel with roles and responsibilities identified in the incident response plan. For example, training staff, validation staff, and evaluation staff.>*
Exercise Facilitator	*<Insert the name of the individual who will lead the discussion among the exercise participants.>*
Data Collector	*<Insert the name of the individual who records information about the actions that occur during the exercise.>*
Date of Testing	*<Insert date and time of testing>*
Location	*<Insert Location>*
Equipment Required	*<Insert required equipment, for example, audio visual equipment, whiteboard, flipchart>*
Material Required	*<Insert required material, for example, participant guides, PowerPoint presentations, handouts>*

Test Scenarios	*<Insert 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.>*
Test Questions	*<Insert a list of questions regarding the scenario that address the exercise objective. Below are sample questions taken from NIST Special Publication 800-61 Computer Security Incident Handling Guide>* **Preparation:** 1. Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate? 2. What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact? **Detection and Analysis:** 1. What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred? 2. What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred? 3. What additional tools might be needed to detect this particular incident? 4. How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process? 5. To which people and groups within the organization would the team report the incident? 6. How would the team prioritize the handling of this incident? **Containment, Eradication, and Recovery:** 1. What strategy should the organization take to contain the incident? Why is this strategy preferable to others? 2. What could happen if the incident were not contained? 3. What additional tools might be needed to respond to this particular incident? 4. Which personnel would be involved in the containment, eradication, and/or recovery processes? 5. What sources of evidence, if any, should the organization acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained? **Post-Incident Activity:** 1. Who would attend the lessons learned meeting regarding this incident? 2. What could be done to prevent similar incidents from occurring in the future? 3. What could be done to improve detection of similar incidents? **General Questions:** 1. How many incident response team members would participate in handling this incident? 2. Besides the incident response team, what groups within the organization would be involved in handling this incident? 3. To which external parties would the team report the incident? When would each report occur? 4. How would each report be made? What information would you report or not report, and why?

	5. What other communications with external parties may occur? 6. What tools and resources would the team use in handling this incident? 7. What aspects of the handling would have been different if the incident had occurred at a different day and time (on-hours versus off-hours)? 8. What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)?
Plan Being Exercise	*<Insert the name and location of the incident response plan being exercised>*
Exercise Agenda	• Introductions • Review Exercise Scope and Logistics • Scenario Walk-Through & review of test questions (Exercise Facilitator) • Data Collector records observations (on-going) • Conduct exercise debrief/hotwash • Exercise Participants released • Complete After-Action Report (Exercise Facilitator & Data Collector only)
Test Plan Approval	*<Insert signature by approval authority (e.g., Business Owner or ISSO)>*

Appendix H. Tabletop Exercise Participant Guide Template

<INSERT ORGANIZATION NAME>

<INSERT TABLETOP EXERCISE TITLE>

PARTICIPANT GUIDE

<Insert Tabletop Location>

<Insert Tabletop Date>

Introduction

In an effort to validate <*insert organization name*> <*insert name of plan being exercised*>, <*insert organization name*> will conduct a tabletop exercise to examine processes and procedures associated with the implementation of the <*insert plan name*>. This discussion-based exercise will be a <*insert number of hours*>-hour event that will begin at <*insert start ti*me> and will last until <*insert end time*>

The exercise is designed to facilitate communication among personnel with incident response roles and responsibilities. The following scenarios have been chosen for this exercise:

- *<Insert scenarios from approved test plan>*

This exercise is designed to improve the readiness of the [insert organization name] and help validate existing <*insert plan name*> procedures.

Participants should come to the exercise prepared to discuss high-level issues related to the incident handling based on the scenarios above. To achieve the exercise's stated objectives, discussion will focus on the following questions related to the scenarios and the incident response plan:

- *<Insert questions from approved test plan>*

Participants may choose to bring incident response narrative or reference material that will aid in answering the above questions.

Concept of Operations

A tabletop exercise is a discussion-based event in which participants meet in a "classroom" setting to address the actions participants would take in response to an emergency. Tabletops are an effective initial step for personnel to discuss the full range of issues related to a crisis scenario. These exercises provide an excellent forum to examine roles and responsibilities, unearth interdependencies, and evaluate plans. A tabletop exercise also satisfies the training requirement for personnel with incident response roles and responsibilities.

Participants will be presented with a incident response. A facilitator will help guide discussion by asking questions designed to address the exercise's objectives.

Objectives

The exercise objectives are as follows:

- *<Insert questions from approved test plan>*

Agenda

Date:	*<Insert date>*
9:00 a.m. – 9:15 a.m.	Introductions
9:15 a.m. – 9:30 a.m.	Review Exercise Scope and Logistics
9:30 a.m. – 11:30 a.m.	Scenario Walk-Through & review of test questions (Exercise Facilitator)
9:30 a.m. – 11:30 a.m.	Data Collector records observations (on-going)
11:30 a.m. – 12:00 p.m.	Conduct exercise debrief/hotwash
Milestone	Exercise Participants released
1:00 p.m. - completion	Complete After-Action Report (Exercise Facilitator & Data Collector only)

Debriefing/Hotwash Questions

An after action report identifying strengths and areas where improvements might be made will be provided after the exercise. The following questions are designed to obtain input into the after action report from participants:

- Are there any other issues you would like to discuss that were not raised?
- What are the strengths of the incident response plan? What areas require closer examination?
- Was the exercise beneficial? Did it help prepare you to execute on your incident response roles and responsibilities?
- What did you gain from the exercise?
- How can we improve future exercises and tests?

Appendix I. After Action Report

<INSERT ORGANIZATION NAME>

<INSERT TABLETOP EXERCISE TITLE>

AFTER ACTION REPORT

<Insert Tabletop Location>

<Insert Tabletop Date>

Introduction

On <*insert date*>, <insert organization name> participated in <*insert duration of exercise*> - hour tabletop exercise designed to validate the organization's understanding of the <*insert plan name.*>

Objectives

The exercise objectives are as follows:

- *<Copy objectives from approved Test Plan>*

Agenda

Date:	*<Insert date>*
9:00 a.m. – 9:15 a.m.	Introductions
9:15 a.m. – 9:30 a.m.	Review Exercise Scope and Logistics
9:30 a.m. – 11:30 a.m.	Scenario Walk-Through & review of test questions (Exercise Facilitator)
9:30 a.m. – 11:30 a.m.	Data Collector records observations (on-going)
11:30 a.m. – 12:00 p.m.	Conduct exercise debrief/hotwash

Milestone	Exercise Participants released
1:00 p.m. - completion	Complete After-Action Report (Exercise Facilitator & Data Collector only)

Discussion Findings

The <*insert exercise name*> provided information on <*insert relevant information*>. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues.

The discussion findings from the exercise along with any necessary recommended actions are as follows:

General Findings

The exercise provided an excellent opportunity for participants to <*insert relevant information*>. As a result of the exercise, participants left with a heightened awareness of <*insert relevant information*>.

Specific Findings

Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:

Observation 1. <*Insert general topic area*>

<*Insert observation*>

Recommendation

<Insert recommendations>

Observation 2. <*Insert general topic area*>

<*Insert observation*>

Recommendation

<Insert recommendations>

Below is an **example** of a completed observation and recommendations, all text in blue should be deleted upon the completion of the After-Action Report.

Example Observations and Recommendations:

Observation 1. Communication

A plan identifying the process for communicating with incident response team members do not exist.

Recommendations:

- The organization should consider developing a communications plan that establishes standardized communications requirements, addresses how stolen documents will be investigated, and describes procedures for personnel incident response team working with organizations to investigate breaches.
- The organization should identify weaknesses in the incident handling plan and procedures to ensure that all essential personnel can be contacted in the event of sensitive document breach.

Observation 2. Incident Breach Handling Protocol

Essential personnel have not been aware of the organization impact of stolen documents, and the incident breach handling protocol to investigation and recovery.

- The agency should examine the criteria for ALL personnel having access to sensitive organization documents. In addition, all personnel might need to attend a security training and awareness course on how to report incidents or suspicious activities.

Appendix J. Incident Scenarios

Scenario 1: Domain Name System (DNS) Server Denial of Service (DOS)

On a Saturday afternoon, external users start having problems accessing the organization’s public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a member of the organization’s networking staff responds to alerts from an Internet border router and determines that the organization’s Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both the organization’s public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

The following are additional questions for this scenario:

1. Whom should the organization contact regarding the external IP address in question?
2. Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?
3. Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

Scenario 2: Worm and Distributed Denial of Service (DDoS) Agent Infestation

On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. The organization has already incurred widespread infections before antivirus signatures become available several hours after the worm started to spread.

The following are additional questions for this scenario:

1. How would the incident response team identify all infected hosts?
2. How would the organization attempt to prevent the worm from entering the organization before antivirus signatures were released?
3. How would the organization attempt to prevent the worm from being spread by infected hosts before antivirus signatures were released?
4. Would the organization attempt to patch all vulnerable machines? If so, how would this be done?
5. How would the handling of this incident change if infected hosts that had received the DDoS agent had been configured to attack another organization’s website the next morning?
6. How would the handling of this incident change if one or more of the infected hosts contained sensitive personally identifiable information regarding the organization’s employees?
7. How would the incident response team keep the organization’s users informed about the status of the incident?

8. What additional measures would the team perform for hosts that are not currently connected to the network (e.g., staff members on vacation, offsite employees who connect occasionally)?

Scenario 3: Stolen Documents

On a Monday morning, the organization’s legal department receives a call from the Federal Bureau of Investigation (FBI) regarding some suspicious activity involving the organization’s systems. Later that day, an FBI agent meets with members of management and the legal department to discuss the activity. The FBI has been investigating activity involving public posting of sensitive government documents, and some of the documents reportedly belong to the organization. The agent asks for the organization’s assistance, and management asks for the incident response team’s assistance in acquiring the necessary evidence to determine if these documents are legitimate or not and how they might have been leaked.

The following are additional questions for this scenario:

1. From what sources might the incident response team gather evidence?
2. What would the team do to keep the investigation confidential?
3. How would the handling of this incident change if the team identified an internal host responsible for the leaks?
4. How would the handling of this incident change if the team found a rootkit installed on the internal host responsible for the leaks?

Scenario 4: Compromised Database Server

On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The team’s investigation determines that the attacker successfully gained root access to the server six weeks ago.

The following are additional questions for this scenario:

1. What sources might the team use to determine when the compromise had occurred?
2. How would the handling of this incident change if the team found that the database server had been running a packet sniffer and capturing passwords from the network?
3. How would the handling of this incident change if the team found that the server was running a process that would copy a database containing sensitive customer information (including personally identifiable information) each night and transfer it to an external address?
4. How would the handling of this incident change if the team discovered a rootkit on the server?

Scenario 5: Unknown Exfiltration

On a Sunday night, one of the organization’s network intrusion detection sensors alerts on anomalous outbound network activity involving large file transfers. The intrusion analyst reviews the alerts; it appears that thousands of .RAR files are being copied from an internal host to an external host, and the external host is located in another country. The analyst contacts the incident response team so that it can investigate the activity further. The team is unable to see what the .RAR files hold because their contents are encrypted. Analysis of the internal host containing the .RAR files shows signs of a bot installation.

The following are additional questions for this scenario:

1. How would the team determine what was most likely inside the .RAR files? Which other teams might assist the incident response team?
2. If the incident response team determined that the initial compromise had been performed through a wireless network card in the internal host, how would the team further investigate this activity?
3. If the incident response team determined that the internal host was being used to stage sensitive files from other hosts within the enterprise, how would the team further investigate this activity?

Scenario 6: Unauthorized Access to Payroll Records

On a Wednesday evening, the organization's physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

The following are additional questions for this scenario:

1. How would the team determine what actions had been performed?
2. How would the handling of this incident differ if the payroll administrator had recognized the person leaving her office as a former payroll department employee?
3. How would the handling of this incident differ if the team had reason to believe that the person was a current employee?
4. How would the handling of this incident differ if the physical security team determined that the person had used social engineering techniques to gain physical access to the building?
5. How would the handling of this incident differ if logs from the previous week showed an unusually large number of failed remote login attempts using the payroll administrator's user ID?
6. How would the handling of this incident differ if the incident response team discovered that a keystroke logger was installed on the computer two weeks earlier?

Scenario 7: Disappearing Host

On a Thursday afternoon, a network intrusion detection sensor records vulnerability scanning activity directed at internal hosts that is being generated by an internal IP address. Because the intrusion detection analyst is unaware of any authorized, scheduled vulnerability scanning activity, she reports the activity to the incident response team. When the team begins the analysis, it discovers that the activity has stopped and that there is no longer a host using the IP address.

The following are additional questions for this scenario:

1. What data sources might contain information regarding the identity of the vulnerability scanning host?
2. How would the team identify who had been performing the vulnerability scans?
3. How would the handling of this incident differ if the vulnerability scanning were directed at the organization’s most critical hosts?
4. How would the handling of this incident differ if the vulnerability scanning were directed at external hosts?
5. How would the handling of this incident differ if the internal IP address was associated with the organization’s wireless guest network?
6. How would the handling of this incident differ if the physical security staff discovered that someone had broken into the facility half an hour before the vulnerability scanning occurred?

Scenario 8: Telecommuting Compromise

On a Saturday night, network intrusion detection software records an inbound connection originating from a watchlist IP address. The intrusion detection analyst determines that the connection is being made to the organization’s VPN server and contacts the incident response team. The team reviews the intrusion detection, firewall, and VPN server logs and identifies the user ID that was authenticated for the session and the name of the user associated with the user ID.

The following are additional questions for this scenario:

1. What should the team’s next step be (e.g., calling the user at home, disabling the user ID, disconnecting the VPN session)? Why should this step be performed first? What step should be performed second?
2. How would the handling of this incident differ if the external IP address belonged to an open proxy?
3. How would the handling of this incident differ if the ID had been used to initiate VPN connections from several external IP addresses without the knowledge of the user?
4. Suppose that the identified user’s computer had become compromised by a game containing a Trojan horse that was downloaded by a family member. How would this affect the team’s analysis of the incident? How would this affect evidence gathering and handling? What should the team do in terms of eradicating the incident from the user’s computer?
5. Suppose that the user installed antivirus software and determined that the Trojan horse had included a keystroke logger. How would this affect the handling of the incident? How would this affect the handling of the incident if the user were a system administrator? How would this affect the handling of the incident if the user were a high-ranking executive in the organization?

Scenario 9: Anonymous Threat

On a Thursday afternoon, the organization’s physical security team receives a call from an IT manager, reporting that two of her employees just received anonymous threats against the organization’s systems. Based on an investigation, the physical security team believes that the threats should be taken seriously and notifies the appropriate internal teams, including the incident response team, of the threats.

The following are additional questions for this scenario:

1. What should the incident response team do differently, if anything, in response to the notification of the threats?
2. What impact could heightened physical security controls have on the team's responses to incidents?

Scenario 10: Peer-to-Peer File Sharing

The organization prohibits the use of peer-to-peer file sharing services. The organization's network intrusion detection sensors have signatures enabled that can detect the usage of several popular peer-to-peer file sharing services. On a Monday evening, an intrusion detection analyst notices that several file sharing alerts have occurred during the past three hours, all involving the same internal IP address.

1. What factors should be used to prioritize the handling of this incident (e.g., the apparent content of the files that are being shared)?
2. What privacy considerations may impact the handling of this incident?
3. How would the handling of this incident differ if the computer performing peer-to-peer file sharing also contains sensitive personally identifiable information?

Scenario 11: Unknown Wireless Access Point

On a Monday morning, the organization's help desk receives calls from three users on the same floor of a building who state that they are having problems with their wireless access. A network administrator who is asked to assist in resolving the problem brings a laptop with wireless access to the users' floor. As he views his wireless networking configuration, he notices that there is a new access point listed as being available. He checks with his teammates and determines that this access point was not deployed by his team, so that it is most likely a rogue access point that was established without permission.

1. What should be the first major step in handling this incident (e.g., physically finding the rogue access point, logically attaching to the access point)?
2. What is the fastest way to locate the access point? What is the most covert way to locate the access point?
3. How would the handling of this incident differ if the access point had been deployed by an external party (e.g., contractor) temporarily working at the organization's office?
4. How would the handling of this incident differ if an intrusion detection analyst reported signs of suspicious activity involving some of the workstations on the same floor of the building?
5. How would the handling of this incident differ if the access point had been removed while the team was still attempting to physically locate it?

Appendix K. Incident Response Reporting Template

Reporters' Contact Information	
Name:	*<insert first, last>*
Phone Number:	*<insert phone number>*
eMail Address:	*<insert eMail address>*
CMS employee or contractor:	
I would like to report the impacted user's contact information, I have the individual consent to do so: <yes> <no>	
Impacted User's Contact Information:	
Name:	*<insert first, last>*
Phone Number:	*<insert phone number>*
eMail Address:	*<insert eMail address>*
CMS employee or contractor?:	
Incident Details	
Time Zone:	*<insert time zone>*
When approximately did the incident start?:	*<insert date, time>*
When was the incident detected?:	*<insert date, time>*
Threat Vectors:	*<insert the threat vectors, i.e., unknown, web, external/removal media, improper usage, email, impersonation/spoofing, loss or theft of equipment, physical cause, attrition, other>*
Is the confidential, integrity, and/or availability of the organization's information system affected? <yes> <no>	
Describe the incident?	*<insert an assessment of the impact>*

What is the affected location and/or name of system?:	*<insert the description>*
What is the estimated number of assets?:	*<insert the number of assets>*
What types of information and data fields are involved?:	*<insert the data fields, e.g., the type of PII, PHI, or FTI involved including (if possible) the specified data fields involved**,** data fields may include name, Social Security Number (SSN), diagnoses, address, phone number, or other attributes that might be used to individually identify the affected persons.>*
What is the estimated number of records involved?:	*<insert the number of records>*
Report (if available and applicable) the following:	
What is the Source Internet Protocol (IP) and Protocol?:	*<insert source of IP>*
What is the Destination IP, Port and Protocol?:	*<insert destination IP>*
What systems functions were affected?:	*<insert the system functions>*
What is the Anti-virus software install (including version, and latest update)?:	*<insert the name of the Anti-virus software>*
What is the method used to identify the incident?:	*<insert method used, e.g., Detection Systems (IDS), audit log analysis, System Administration>*
Did an incident occur at a contractor hosted or managed site?:	*<yes> <no>*

Appendix L. Incident Response Plan Template

<table>
<tr><th colspan="2">Purpose</th></tr>
<tr><td colspan="2">The objective of this Incident Response Plan (IRP) is to outline the incident handling and response process for the <*system name*> in accordance with the requirements outlined in the CMS Acceptable Risk Safeguards (ARS) and CMS Risk Management Handbook (RMH) Chapter 8, Incident Response. This plan covers all assets within the information system boundary, transmitting, storing, or processing CMS information. Furthermore, this plan describes how to manage incident response according to all Federal, Departmental and Agency requirements, policies, directives, and guidelines.</td></tr>
<tr><td><b>Scope</b></td><td>This IRP is written for the <*system name*> stakeholders with incident response roles and responsibilities and describes those responsibilities for each phase of the incident life cycle. This plan establishes a quick reference for security and privacy incident handling and response.</td></tr>
<tr><td><b>Definitions</b></td><td>The following key terms and definitions relate to incident response:
<b>Administrative Vulnerability:</b> An administrative vulnerability is a security weakness caused by incorrect or inadequate implementation of a system’s existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency. It is characterized by the fact that the full correction of the vulnerability is possible through a change in the implementation of the system or the establishment of a special administrative or security procedure for the system administrators and users. Poor passwords and inadequately maintained systems are the leading causes of this type of vulnerability.
<b>Breach:</b> A breach is an incident that poses a reasonable risk of harm to the applicable individuals. For the purposes of Office of Management and Budget (OMB) OMB M-07-16 (for PII incidents) and Health Information Technology for Economic and Clinical Health (HITECH) Act (for PHI incidents) reporting requirements, a privacy incident does not rise to the level of a breach until it has been determined that the use or disclosure of the protected information compromises the security or privacy of the protected individual(s) and poses a reasonable risk of harm to the applicable individuals. For any CMS privacy incident, the determination of whether it may rise to the level of a breach is made (exclusively) by the CMS Breach Analysis Team (BAT), which determines whether the privacy incident poses a significant risk of financial, reputational, or other harm to the individual(s).
<b>Event:</b> 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.
<b>Federal Tax Information (FTI):</b> Generally, 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.</td></tr>
</table>

Incident Response: Incident response outlines steps for reporting incidents and lists actions to be taken 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.

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

Security Incident: In accordance with *NIST 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 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

	Technical Vulnerability: A technical vulnerability is a hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally, thus increasing the risk of compromise, alteration of information, or denial of service.
Roles and Responsibilities	
<Insert the roles and responsibilities associated with this plan. Possible roles include: • *Business Owners:* • *Information System Owner(s)* • *Cyber Risk Advisors (CRA)* • *Information System Security Officer (i.e., ISSO)* • *CCIC Incident Management Team (i.e., CCIC IMT)* *For a detailed description of the responsibilities associated with these role please refer to the CMS IS2P2 located at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS2P2.pdf>*	
Understanding an Incident	
The following lists a small subset of common well known incidents:	
Types of Incidents	• **Data Destruction or Corruption:** The loss of data integrity can take many forms including changing permissions on files making the files writable by non-privileged users, deleting data files and or programs, changing audit files to cover-up an intrusion, changing configuration files that determine how and what data is stored and ingesting information from other sources that may be corrupt • **Data Compromise and Data Spills:** Data compromise is the exposure of information to a person not authorized to access that information either through clearance level or formal authorization. This could happen when a person accesses a system not authorized to access or through a data spill. Data spill is the release of information to another system or person not authorized to access that information, even though the person is authorized to access the system on which the data was released. This can occur through the loss of control, improper storage, improper classification, or improper escorting of media, computer equipment (with memory), and computer generated output • **Malicious Software (Malware):** Malicious code is software based attacks used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem. The following is a brief listing of various software attacks: 1. **Virus:** It is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data). 2. **Worm:** An unwanted, self-replicating autonomous process (or set of processes) that penetrates computers using automated hacking techniques.

	3. **Trojan Horse:** A useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data. 4. **Spyware:** Surreptitiously installed malicious software that is intended to track and report the usage of a target system or collect other data the author wishes to obtain. 5. **Rootkit Software:** Software that is intended to take full or partial control of a system at the lowest levels. Contamination is defined as inappropriate introduction of data into a system. 6. **Privileged User Misuse:** Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains. 7. **Security Support Structure Configuration Modification:** Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled. SSS' are essential to maintaining the security policies of the system Unauthorized modifications to these configurations can increase the risk to the system. **Note: These categories of incidents are not necessarily mutually exclusive.**
Causes of Incidents	• **Malicious Code:** Malicious code is software or firmware intentionally inserted into an information system for an unauthorized purpose • **System Failures:** Procedures Failures or Improper Acts. A secure operating environment depends upon proper operation and use of systems. Failure to comply with established procedures, or errors/limitations in the procedures for a CMS system, can damage CMS reputation and increase vulnerability/risk to the system or application. While advances in computer technology enable the building of increased security into the CMS architecture, much still depends upon the people operating and using the system(s). Improper acts may be differentiated from insider attack according to intent. With improper acts, someone may knowingly violate policy and procedures, but is not intending to damage the system or compromise the information it contains • **Intrusions or Break-Ins:** An intrusion or break-in is entry into and use of a system by an unauthorized individual • **Insider Attack:** Insider attacks can provide the greatest risk. In an insider attack, a trusted user or operator attempts to damage the system or compromise the information it contains
Avenues of Attack	As with any information system, attacks can originate through certain avenues or routes. An attack avenue is a path or means by which an attacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack avenues enable attackers to exploit system vulnerabilities, including the human element. If a system were locked in a vault with security personnel surrounding it, and if the system were not connected to any other system or network, there would be virtually no avenue of attack. However, there are numerous avenues of attack. • Local and/or partner networks • Unauthorized devices (including non-approved connections to a local network) • Gateways to outside networks • Communications devices

- Shared disks
- Removable media
- Downloaded software
- Direct physical access

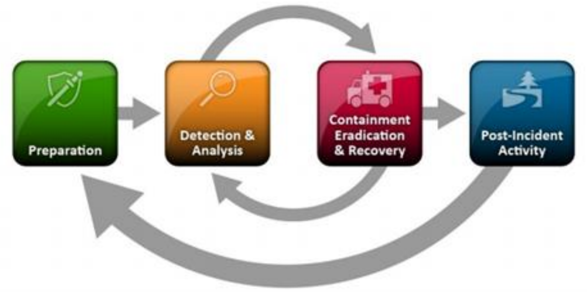
Possible Impacts of an Attack

One of the major concerns of a verifiable computer security attack is that sensitive PII is compromised. The release of sensitive information to people without the proper need-to-know or formal authorization jeopardizes the tenant of Confidentiality, Integrity and Availability (CIA). In addition, users may lose trust in computing systems and become hesitant to use one that has a high frequency of incidents or even a high frequency of events that cause the user to distrust the integrity of the federal system. Moreover, users become disenfranchised with any action that causes all or part of the network's service to be stopped entirely, interrupted, or degraded sufficiently to impact operations; as with a DoS attack. The list of impacts from attacks that compromise computer security include:

- Denial of Service
- Loss or Alteration of Data or Programs
- Privacy Incident, including those resulting in identity theft or data breach
- Loss of Trust in Computing Systems
- The loss of intellectual property and CMS confidential information
- Reputational damage to the organization
- The additional cost of securing networks, insurance, and recovery from attacks

Incident Life Cycles

The incident response process has four phases. The diagram below illustrates the four phases of the NIST 800-61 Incident Lifecycle:



Preparation

Preparation ensures that the organization is ready to respond to incidents, but can also prevent incidents by ensuring that systems, networks, and applications are sufficiently secure. The following describes the techniques utilized by the <*system name*> and to prepare for security and privacy incidents.

<Describe the activities and methods in place for the information system to prepare for information security incidents. Examples of preparation methods are, implementing incident response tools, establishing security baselines, and running periodic announced training and/or unannounced drills. For additional information on preparation activities please review Section 3.3.1 Preparation of the CMS RMH Chapter 8 Incident Response.>

<Describe how incidents involving PII are to be handled, including the policies and procedures that have been developed and how those policies and procedures are communicated to the staff. Staff should be informed of the consequences of their actions for inappropriate use and handling of PII. Describe how it is determined

	that the existing processes are adequate and that staff understand their responsibilities. Describe how suspected or known incidents involving PII are reported to the business owner, information system owner, CRA, ISSO, and CCIC IMT. Describe what information needs to be reported, and to whom.>
Detection and Analysis	Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies. The following section describes the techniques utilized by the <system name> to detect and analyze security incidents *<Describe the activities and methods in place for the information system to detect and analyze for information security incidents. Examples of detection and analysis methods are, prepare for common attack vectors, recognize the signs of an incident, and document and prioritize the incident. For additional information on preparation, activities please review Section 3.3.2 Detection and Analysis of the CMS RMH Chapter 8 Incident Response.>* *<Describe the activities and methods in place to detect and analyze incidents involving PII that are the responsibility of the information staff. Describe how it is ensured that the analysis process includes an evaluation of whether an incident involved PII, focusing on both known and suspected breaches of PII. Detection of an incident involving PII also requires reporting internally, to US-CERT, and externally, as appropriate; this is a CCIC IMT responsibility.>*
Containment, Eradication & Recovery	**Containment** Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making. Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. The following section describes the containment strategies and procedures for the <*system name*>: *<Describe the strategies and procedures in place for the information system to contain information security incidents. Examples of containment strategies are, shut down a system, disconnect it from a network, and/or disable certain functions. For additional information on Containment activities, review Section 3.3.3 Containment, Eradication and Recovery of the CMS RMH Chapter 8 Incident Response.>* *<Describe the strategies and procedures in place for containing incidents involving PII.>* **Eradication and Recovery** After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that the hosts can be remediated. For some incidents, eradication is either not necessary or is performed during recovery. *<Describe the activities and methods in place for the information system to eradicate and recover from information security incidents. Examples methods for*

	eradication are delete malware, disable breached accounts, identify and mitigate vulnerabilities that were exploited. Examples activities associated with recovering from information security incidents are restore systems to normal operation, confirm that systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. For additional information on Eradication and Recovery activities review Section 3.3.3 Containment, Eradication and Recovery of the CMS RMH Chapter 8 Incident Response.> *<Describe if media sanitization steps are performed when PII needs to be deleted from media during recovery. PII should not be sanitized until a determination has been made about whether the PII must be preserved as evidence. Describe if forensics techniques are needed to ensure preservation of evidence. If PII was accessed, how is it determined how many records or individuals were affected. These activities should be coordinated with the CCIC IMT.>*
Post-Incident Activity	After an incident has been eradicated and recovery completed, each incident response team should evolve to reflect upon new threats, improve technology, and document lessons learned. Holding a lessons learned meeting with all involved parties after a major incident, and optionally after lesser incidents, can be extremely helpful in improving information security measures and the incident handling process. *<Describe the activities and methods in place for the information system to conduct post-incident activity after information security incidents. Examples methods for post-incident activity are: to conduct a lesson learned meeting, document the lessons learned, update the IRP and associated procedures as necessary, and ensure evidence is retained and archived. For additional information on post-incident activity review Section 3.3.4 Post-Incident Activity of the CMS RMH Chapter 8 Incident Response.>* *<Describe the activities and methods in place to conduct post-incident activity after incidents involving PII. This should include how the IRP is continually updated and improved based on the lessons learned during each incident. Sharing information within CMS and US-CERT to help protect against future incidents is a CCIC responsibility.>*
Reporting Requirements	
<Describe the information system process for reporting information security incidents. Incident should be reported to the CMS IT Service Desk within one hour, by calling at (410) 786-2580 (i.e., internal) or (1-800) 562-1963 (internal and external) or email CMS_IT_Service@cms.hhs.gov. For information on reporting requirements *for information security and privacy incidents,* review Section 3.5 Incident Reporting and Appendix K for the Incident Response Reporting Template in *The CMS RMH Chapter 8 Incident Response*.>	
Points of Contact	
Business Owner *<insert name>* *<insert email>* *<insert phone>* **CMS IT Service Desk** *<insert name>*	

<insert email>
<insert phone>

Cybersecurity Risk Advisor (CRA)

<insert name>
<insert email>
<insert phone>

Data Guardian

<insert name>
<insert email>
<insert phone>

Incident Management Team

<insert name>
<insert email>
<insert phone>

Incident Responders

<insert name>
<insert email>
<insert phone>

Information System Security Officer (ISSO)

<insert name>
<insert email>
<insert phone>

System Administrators

<insert name>
<insert email>
<insert phone>

System Developers

<insert name>
<insert email>
<insert phone>

Plan Approval

Business Owner (BO)

<insert signature>
<insert name>

<insert title>
<insert email>
<insert phone>

Information System Security Officer (ISSO)

<insert signature>
<insert name>
<insert title>
<insert email>
<insert phone>

Appendix M. Incident Preparation Checklist

Incident Preparation Checklist		
Activity	**Description**	**Status**
Preparation (Communications and Facilities):		
Contact Information	Ensure that contact information for team members and others outside of the organization (primary and backup contacts) is maintained in the Incident Response Plan (IRP). Information should include phone numbers, email addresses, public encryption keys, and instructions for verifying the contacts identity.	<Not Started, In Progress, Completed, N/A>
On Call Information	Ensure on-call information for teams within the organization is documented in the IRP, including escalation information.	<Not Started, In Progress, Completed, N/A>
Incident Reporting Mechanisms	Ensure that information such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents are included in the IRP.	<Not Started, In Progress, Completed, N/A>
Issue Tracking System	Ensure that a system exists for tracking incident information, status, etc.	<Not Started, In Progress, Completed, N/A>
Encryption Software	Identify encryption software to be used for communications among team members within the organization and for external parties. Software must use FIPS validated encryption. The current approved software package for CMS is SecureZip.	<Not Started, In Progress, Completed, N/A>
War Room	Ensure that a war room exists for centralized communication and coordination. A permanent war room is not necessary but procedures should exist within the IRP for preparing a temporary war room when needed.	<Not Started, In Progress, Completed, N/A>
Secure Storage Facility	Identify a secure storage facility for securing evidence and other sensitive materials.	<Not Started, In Progress, Completed, N/A>
Preparation (Incident Analysis and Software):		
Digital Forensic Workstations	Ensure that digital forensic workstations are available to create disk images, preserve log files, and save other relevant incident data.	<Not Started, In Progress, Completed, N/A>

Incident Preparation Checklist		
Activity	**Description**	**Status**
Laptops	Ensure that laptops are available for activities such as analyzing data, sniffing packets, and writing reports.	<Not Started, In Progress, Completed, N/A>
Spare Workstations, Servers, and Networking Equipment or Virtualized Equivalents	Ensure that spare workstations, servers, and networking equipment or virtualized equivalents are available. This equipment may be used for many purposes, such as restoring backups and trying out malware.	<Not Started, In Progress, Completed, N/A>
Blank Removable Media	Ensure access to blank removable media. This media may be used to maintain copies forensic data or incident artifacts.	<Not Started, In Progress, Completed, N/A>
Portable Printer	Ensure access to a portable printer to print copies of log files and other evidence from non-networked systems.	<Not Started, In Progress, Completed, N/A>
Packet Sniffers and Protocol Analyzers	Ensure packet sniffers and protocol analyzers are available to capture and analyze network traffic.	<Not Started, In Progress, Completed, N/A>
Digital Forensic Software	Ensure digital forensic software is available to analyze disk images.	<Not Started, In Progress, Completed, N/A>
Removable Media	Ensure removable media is available with trusted versions of programs to be used to gather evidence from systems.	<Not Started, In Progress, Completed, N/A>
Evidence Gathering Accessories	Ensure evidence gathering accessories are on hand and available including hardbound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions.	<Not Started, In Progress, Completed, N/A>
Port List	Ensure a list exists and is ready available that documents the commonly used ports, protocols, and services.	<Not Started, In Progress, Completed, N/A>

Incident Preparation Checklist		
Activity	**Description**	**Status**
Documentation	Ensure documentation is maintained and available for operating systems, applications, protocols, and intrusion detection and antivirus products.	<Not Started, In Progress, Completed, N/A>
Network Diagrams	Ensure that a network diagrams are maintained and available, and ensure a list of critical assets are included, such as database servers.	<Not Started, In Progress, Completed, N/A>
Current Baselines	Ensure that baselines are maintained documenting the expected network, system, and application activity.	<Not Started, In Progress, Completed, N/A>
Access to Images	Ensure that images of clean operating system and application installations are available for recovery purposes.	<Not Started, In Progress, Completed, N/A>

Appendix N. Points of Contact

CMS IT Service Desk

Name	Email	Phone
CMS IT Service Desk	CMS_IT_Service_Desk@cms.hhs.gov	(410) 786-2580 (800) 562-1963

Incident Management Team

Name	Email	Phone
Incident Management Team	IncidentManagement@cms.hhs.gov	(443) 537-9713

Appendix O. Feedback and Questions

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