Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Risk Management Handbook (RMH)
Chapter 08: Incident Response

Final

Version 2.0

July 10, 2020

Record of Changes

The table below capture changes when updating the document. All columns are mandatory.

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
1.0	01/31/2017	All	CMS ISPG	Initial publication
1.1	06/29/2017	Appendix F and K	CMS ISPG	Added additional Category Severity Levels to Appendix F. Updates reflect the latest US-CERT reporting requirements The Appendix K Template is referenced, but has been moved outside of the document to the Information Security and Privacy Library. All referenced links to Appendix K have been moved out of the document and onto the ISP Library.
2.0	03/30/2020	All	CMS ISPG	Updated Procedures, referenced HHS Privacy Breach Policy and CISO Playbook, Added IR-04(4), Removed controls IR-03(1);IR-04(1),(3),(7),(8); IR-07(2); IR-09(1),(2),(3),(4); IR-10. Templates have been removed from the document and onto the ISP Library with referenced links.
2.0	04/21/2020	Introduction, Apendixes, Roles & Responsibilities, Standards, Policy.	CMS ISPG	Deleted sections Introduction, Policy, Standards, Roles & Responsibilities, HIPAA Integration and Appendixes. We have documents which address all these sections (JBH Review RMH Preface & RMH Appendixes)

Effective Date/Approval

This Procedure becomes effective on the date that CMS's Director, Division of Security and Privacy Policy and Governance (DSPPG) signs it and remains in effect until it is rescinded, modified or superseded.

Signature:	Michael E. Pagels -S Digitally signed by Michael E. Pagels -S Date: 2020.07.15 16:21:41 -04'00'	Date of Issuance	
	Michael Pagels Director, Division of Security and Privacy Policy and Governance (DSPPG) and Acting Senior Official for Privacy		

Table of Contents

Summary of Changes ..... **ii**

Effective Date/Approval ..... **iii**

Table of Contents ..... **iii**

1. Executive Summary **6**

2. Common Control Inheritance **6**

3. Procedures **7**

3.1 Incident Response Training (IR-02) 7

3.1.1 Simulated Events (IR-02(01)) 9

3.1.2 Automated Training Environments (IR-02(02)) 10

3.2 Incident Response Training (IR-03) 10

3.2.1 Coordination with Related Plans (IR-03(02)) 12

3.3 Incident Handling (IR-04) 12

3.3.1 Preparation 14

3.3.2 Detection and Analysis 16

3.3.3 Containment, Eradication and Recovery 24

3.3.4 Post-Incident Activity 25

3.3.5 Automated Incident Handling (IR-04(01)) 25

3.3.6 Information Correlation (IR-04(04)) 26

3.4 Incident Monitoring (IR-05) 26

3.4.1 Automated Tracking/Data Collection/Analysis (IR-05(01)) 27

3.5 Incident Reporting (IR-06) 27

3.5.1 Automated Reporting (IR-06(01)) 29

3.6 Incident Response Assistance (IR-07) 29

3.6.1 Automation Support for Availability of Information/Support (IR-07(01)) 29

3.7 Incident Response Plan (IR-08) 30

Appendix A. Incident Response Plan Template **32**

Tables

Table 1: CMS Defined Parameters – Control IR-028
Table 2: CMS Defined Parameters – Control IR-03……..11
Table 3: Common Sources of Precusors and Indicators 17
Table 4: Automated Tools 24
Table 5: CMS Defined Parameters – Control IR-06..... 26
Table 6: CMS Defined Parameters – Control IR-08..... 28

Figures

Figure 1: Incident Response Life Cycle …….....12

1. Executive Summary

RMH Chapter 8 Incident Response documents the controls that focus on how the organization must: establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate organizational officials and/or authorities. Procedures addressed include incident response training, incident response testing, incident handling, monitoring and reporting, and information spillage response. Within this chapter, readers will find the CMS Cybersecurity Integration Center (CCIC) Functional Area Overview figure and how the Incident Management Team (IMT) within the CCIC works with systems to mitigate information security and privacy incidents.

Supplements that can be located in the Information Security and Privacy Library (ISPL) are:

- Tabletop Exercise template
- Incident Preparation Checklist
- Incident Response Reporting template
- Incident Response Plan template

2. Common Control Inheritance

The inherited controls list can be used to identify common controls offered by system alternatives. The use of inherited controls is optional, the objective of this process is to identify opportunities to extract benefits (and reduce costs) by maximizing the use of already existing solutions, and minimizing duplication of efforts across the enterprise.

Below is a listing of controls that can be inherited, where they can be inherited from and if they are a hybrid control for this control family.

Incident Response Control	Inheritable From	Hybrid Control
IR-01	OCISO Inheritable Controls	Yes
IR-02	CMS Baltimore Data Center - EDC4	No
IR-02(01)	CMS Baltimore Data Center - EDC4	No
IR-02(02)	CMS Baltimore Data Center - EDC4	No
IR-03	CMS Baltimore Data Center - EDC4	No
IR-03(01)	CMS Baltimore Data Center - EDC4	No

Incident Response Control	Inheritable From	Hybrid Control
IR-03(02)	CMS Baltimore Data Center - EDC4	No
IR-04	CMS Baltimore Data Center - EDC4	No
IR-04(01)	CMS Baltimore Data Center - EDC4	No
IR-04(04)	CMS Baltimore Data Center - EDC4	No
IR-05	CMS Baltimore Data Center - EDC4	No
IR-05(01)	CMS Baltimore Data Center - EDC4	No
IR-06	CMS Baltimore Data Center - EDC4	No
IR-06(01)	CMS Baltimore Data Center - EDC4	No
IR-07	CMS Baltimore Data Center - EDC4	No
IR-07(01)	CMS Baltimore Data Center - EDC4	No
IR-08	CMS Baltimore Data Center - EDC4	No
IR-09	CMS Baltimore Data Center - EDC4	No
IR-09(01)	CMS Baltimore Data Center - EDC4	No
IR-09(02)	CMS Baltimore Data Center - EDC4	No
IR-09(03)	CMS Baltimore Data Center - EDC4	No
IR-09(04)	CMS Baltimore Data Center - EDC4	No

3. Procedures

Procedures assist in the implementation of the required security and privacy controls.

In this section, the IR family procedures are outlined. To increase traceability, each procedure maps to the associated National Institute of Standards and Technology (NIST) controls using the control number from the CMS Acceptable Risk Safeguards (ARS).

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 Federal Information

Security Modernization Act (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 Information System Owners (SO), Business Owners (BO), 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 to carry out the CMS mission receive incident response training annually as part of the general information security awareness training.

The CMS Chief Information Officer (CIO), CMS Chief Information Security Officer (CISO), and the CMS Senior Official for Privacy (SOP) shall endorse and promote an organizational-wide information systems security and privacy awareness training. According to CMS Information Systems Security and Privacy Policy (IS2P2) Section 2.2, the 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 CISO and the SOP 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 FTI provide appropriate safeguard measures to ensure the confidentiality of the FTI. Incident response training is one of the safeguards for implementing this requirement.

The CMS Information Security and Privacy Group (ISPG) will provide incident response training to information system users that 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 SOP.

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

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; b. When required by information system changes; and	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) When required by information system changes; and

Control	Control Requirement	CMS Parameter
	c. [*Assignment: organization-defined frequency*] thereafter	c) Within every three hundred sixty-five (365) days thereafter

3.1.1 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 Information Systems Security and Privacy Awareness Training. All EUA users must take the CBT Training located at CMS Information Technology Security and Privacy web pageThe training will be delivered to all EUA users initially prior to account issuance and annually thereafter. It is the responsibility of users to take this training within three (3) days.
- **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 **.**

3.1.2 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.

3.1.3 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.[1]

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 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 that 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), adaptive capabilities testing (ACT) or existing Plan of Action and Milestones (POA&Ms) might assist in selecting scenarios for

[1] See NIST SP 800-84 – *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, and NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*

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). Detailed descriptions of each of these scenarios can be found in the ISPL (Information Security and Privacy Library) and the scenarios are 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 Automated Training Environments (IR-02(02)).

3.1.4 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-03

Control	Control Requirement	CMS Parameter
IR-03	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	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 organization's incident response effectiveness, and documents its findings.

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 located in the ISPL as part of the *"TableTop Exercise Template***.** 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 located in the ISPL as part of the *"TableTop Exercise Template"*. For more information on functional exercise material please refer to Section 5.3 of NIST SP 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 the ISPL as part of the *"TableTop Exercise Template"*. This step is completed by the Exercise Facilitator and Data Collector.

3.2.1 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

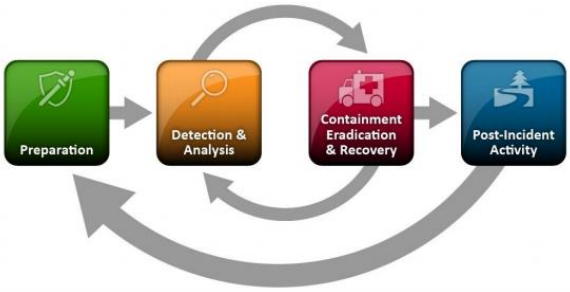
The following steps detail the CMS specific process to ensure Coordination with Related Plans:

- **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 1: Incident Response Life Cycle



All distributed Incident Response Teams (IRT) fall under the authority of the 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.

In the event of a suspected or confirmed privacy (PII) data breach, CCIC IMT will notify ISPG that a Breach Analysis Team (BAT) should be convened, including representatives from ISPG, IMT, and system stakeholders such as the system Business Owner. The BAT will conduct and document a formal Risk Assessment to assess the risk of harm to individuals potentially affected by the breach. The following factors are used:

- Nature and sensitivity of PII
- Likelihood of access and use of PII and
- Type of breach

If the Risk Assessment concludes that there is a moderate or high risk that PII has been compromised, the CMS Senior Official for Pivacy will work with IMT and system stakeholders to develop a notification plan to notify affected individuals and mitigate their risk.

Affected individuals should be notified of a breach via first-class mail where possible, though depending on the nature and scale of the breach, additional methods such as email, telephone, and local media outreach may be used. The breach notification should include the following information:

- Source of the breach
- Brief description
- Date of discovery and breach occurrence
- Type of PII involved
- A statement whether or not the information was encrypted
- What steps individuals should take to protect themselves from potential harm and services being provided to potentially affected individuals
- What the agency is doing to investigate and resolve the breach
- Who affected individuals should contact for information

In addition to breach notification, CMS must also consider how best to mitigate the risk of harm to affected individuals. CMS may need to provide:

- Countermeasures against misuse of lost PII/PHI, such as notifying a bank if credit card numbers are lost
- Guidance on how affected individuals can protect themselves against identity theft, such as education on credit freezes and other defensive measures
- Services, such as credit monitoring

The Breach Analysis Team may determine that some, all, or none of these mitigation techniques are appropriate for a given breach. Some breaches may require notification, but not mitigation.

The SOP coordinates with HHS Privacy Incident Response Team (PIRT) for review and approval of CMS response plan, breach notification, and breach mitigation. 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:

Steps	Activity
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 the ISPL. 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

Steps	Activity

	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.

Steps	Activity
	• **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 Information Systems Security and Privacy Awareness Training. All EUA users must take the CBT Training located at CMS Information Technology Security and Privacy web page. 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

Steps	Activity
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:

Steps	Activity
	• **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

Alerts

Source	Description
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

Source	Description
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.

Source	Description
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 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

Source	Description
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

Source	Description
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.

Steps	Activity
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

Steps	Activity
	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

Steps	Activity
	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.

Steps	Activity
	• **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 (Computer Security Incident Response Teams), 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:	• Continue to document updates to the incident in the Incident Response Reporting Template form.
Step 5	• Prioritize the incident using the criteria found in the *"Impact Category, Attack Vector Descriptions, & Attribute Category"* document which is located in the ISPL
Step 6	• Establish communication method and notify the appropriate CMS personnel. *The Incident Notification Table,* located in the Incident Response Steps for CISO (CISO Playbook) document, is a guide on notification steps per incident type. in the The list below provides examples of individuals that may require notification in the event of an incident: • CIO • CISO • Deputy CISO • SOP • HHS Office of the Inspector General (OIG) • Local information response team within the organization • External incident response team (if appropriate) • System Owner • Information System Security Owner • System Business Owner

Steps	Activity
	• System Cyber Risk Advisor • System Data Guardian • CMS Office of Human Capital (for cases involving employees, such as harassment through email) • CMS Office of Financial Management (in the case where extra funding is needed for investigation activities) • CMS Office of Communications (for incidents that may generate publicity) • CMS Office of Legislation (for incidents with potential legal ramifications) • US-CERT (required for Federal agencies and systems operated on behalf of the Federal government). • Individual (whose PII has been compromised)

The below table documents the responsibilities that should be fulfilled by employees in certain roles during an incident response event

Role	Responsibility
CISO	• Lead the investigation and resolution of information security and privacy incidents and breaches across CMS. • Once an incident has been validated, the incumbent CISO will follow the steps in the *CISO Playbook*. This playbook details the CISO's responsibilities, the scenarios to be considered and the relevant incident response contacts during an event.
IMT Lead	• Notify and deliver incident situation reports to CMS CISO. • Coordinate Incident Response activities
Senior Official for Privacy (SOP)	• Coordinate/Support incident response activities with CISO. • In the event of a PII/PHI breach, coordinate with the system Business Owner and HHS PIRT to handle notifying affected individuals • Provide overall direction for incident handling which includes all incidents involving PII/PHI.
Business Owner	• Works with IMT Lead to coordinate incident response activities related to their assigned CMS information systems. • In the event of a PII/PHI breach, coordinate with the Senior Official for Privacy and HHS PIRT to handle notifying affected individuals
CMS IT Service Desk	• Notify IMT of incident situation

Role	Responsibility
	• Ensure Incident Response form has been completed as accurately as possible at the time of the initial report.
Designated Appointee	• Update the ServiceNow ticket as the situation arises and follow up with the CMS IT Helpdesk until incident has been resolved.

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. 2 *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. The following table provides examples of tools used for automated incident handling processes at CMS.

Table 4: Automated Tools

Tools	Description	Users
HHS RSA Archer	The HHS tool used for all incident/tracking and reporting. Users do not access HHS Archer directly.	CCIC IMT and CCIC SOC Analysts
ServiceNow	The CMS ServiceNow 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 Information Correlation (IR-04(04))

The purpose of Information Correlation is to ensure that CMS correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. To achieve this,

1. All tickets submitted in ServiceNow are thoroughly worked through to determine the validity of being classified as an incident. The submitted tickets are correlated and analyzed for trends.
2. CCIC uses the SIEM tool, Splunk, to correlate data from various sources to receive alerts associated with incident breaches.

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. One of such services is Continuous Diagnostics and Mitigation (CDM), which is still in development and not all data centers have been transitioned. Other services include vulnerability management, security engineering, incident management, forensics and malware analysis, information sharing, cyber-threat intelligence, penetration testing, and software assurance.

The IMT is the group responsible for tracking and documenting security and privacy incidents. Stakeholders outside of the IMT (e.g., incident responders, ISSO, system owners, etc.) are responsible for providing the information necessary to track and monitor information security and privacy 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 Archer/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.

- CMS uses a ServiceNow ticketing system for all privacy and security incidents for incident/tracking and reporting.
- The CMS ServiceNow ticket is used by the CMS IT Service Desk to track changes and problems within the CMS environment.
- The HHS Archer is the incident response tool used to notifiy HHS of an incident. A shell ticket is automatically created in HHS Archer when CMS IMT is assigned a ticket in ServiceNow.
- The CCIC IMT updates the incident information in ServiceNow which will post automatically to HHS Archer. This will occur till the incident has been resolved.
- CMS RSA Archer/CFACTS SecOps Module is used for investigating potential incidents discovered by the CCIC SOC.

3.5 Incident Reporting (IR-06)

The intent of this control is to ensure that CMS requires employees and contractors to report suspected or confirmed 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 5: 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] b. Reports security, privacy and supply chain incident information to [Assignment: organization-defined authorities]	The organization: a. Requires personnel to report actual or suspected security and privacy incidents to the organizational incident response capability within 1 hour of discovery/notification; and b. Reports security, privacy and supply chain incident information to CMS IT Service Help Desk.

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

- **Step 1:** Report the suspected information security and privacy incident to the CMS IT Service Desk at (410) 786-2580 (internal only) or (800) 562-1963 (internal and external) and/or email CMS_IT_Service@cms.hhs.gov. Additionally, contact your ISSO as soon as possible and apprise them of the situation. All suspected information security and privacy incidents must be reported to the CMS IT Service Desk within one hour of discovery.
- **Step 2:**After notifiying the CMS IT Service Desk, collect as much supporting information as possible on the suspected security and privacy incident using the Incident Response Reporting Template located in the ISPL. Provide the information contained on the completed incident reporting form to the CMS IT Service Desk.

  Note: *This template replaces the previous HHS CMS Computer Security Incident Report form that was published separately to the information security library.*
- **Step 3:**The CMS IT Service Desk creates a ServiceNow ticket and enters the details on the suspected security and privacy incident. This ServiceNow ticket creates a shell ticket in HHS Archer, which is the HHS incident response tool.
- **Step 4:**The IMT will update the ServiceNow ticket, as necessary, which will automatically populate in HHS Archer until the incident has been resolved.
- **Step 5:** 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 information security incident.
- **Step 2:** The CMS IT Service Helpdesk will open a ServiceNow ticket and record the incident. This ServiceNow ticket automatically generates an Archer ticket notifying HHS CSIRC.
- **Step 3:** The CMS IT Service Helpdesk will then assign the ticket to the IMT and they will evaluate the incident report while providing updates to CMS CISO and HHS CSIRC.
- **Step 4:** The user (reporter) will continue to update the incident report in ServiceNow or contact the CMS IT Service Helpdesk.
- **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.
- **Step 7:** The user (reporter) will work with the IMT until remediation of the security incident.

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, 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 online libraries.

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

- The CMS website

- The CMS CISO mailbox at CISO@cms.hhs.gov
- CMS IT Service Desk at CMS_IT_Service@cms.hhs.gov
- CMS Incident Management Team (IMT) at IncidentManagement@cms.hhs.gov
- The CMS Intranet (this service is available ONLY to personnel who have access to a GFE issued device, (i.e., laptop, desktop))
- The HHS.gov
- The HHS Intranet (this service is available ONLY to personnel who have access to a GFE issued device, (i.e., laptop, desktop))

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 4.2.8 of this handbook. The Incident Response Plan template is attached to this document as Appendix A. 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 6: 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];	a. Incident Response Plan is reviewed and approved by the applicable Business Owner at least annually.

Control	Control Requirement	CMS Parameter
	b. Distributes copies of the incident response plan to [Assignment organization-defined incident response personnel (identified by name and/or role) and organizational elements] c. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; d. 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	b. Distributes copies of the incident response plan to CMS CIO, CMS CISO, ISSO, CMS OIG Computer Crime Unit (CCU), All personnel within the CMS Incident Response Team, PII Breach Response Team and Operations Centers. c. Reviewed annually updated as required d. Communicates incident response plan changes to all stakeholders.

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:

- **Step 1:** Complete a draft IRP by leveraging the template and instructions located in Appendix A.
- **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.

Appendix A: Incident Response Plan Template

Purpose
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.

Scope
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.

Definitions
The following key terms and definitions relate to incident response: **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. **Breach:** 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-17-12 (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). **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. **Federal Tax Information (FTI):** 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

Definitions
maintaining appropriate safeguards to protect the information confidentiality. [IRS 1075] Tax return information that is not provided by the IRS falls under PII. **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 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 **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/Info-Security-Library-Items/CMS-Information-Systems-Security-and-Privacy-Policy-IS2P2*

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.

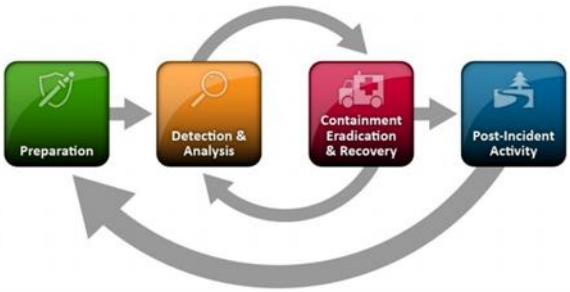
Types of Incidents
4. **Spyware:** Surreptitiously installed malicious software that is intended to track and report the usage of a target system or collect other data the author wishes to obtain. 5. **Rootkit Software:** Software that is intended to take full or partial control of a system at the lowest 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

Avenues of Attack
• 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 SP 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*

Preparation
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**

Containment, Eradication & 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 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>*

Points of Contact
<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>*