DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Enterprise Architecture Strategy Group (EASG)

CMS Information Security Incident Handling and Breach Analysis/Notification Procedure

Version 2.0
August 16, 2007

Summary of changes in Incident Handling Procedure version 2.0

The most significant changes to the document are:

1. The document name has been changed to include “Breach Analysis/Notification”.
2. This is a complete rewrite of the Incident Handling Procedures due to new guidance from the Department of Health and Human Services (DHHS). This document adopts verbatim many definitions, incident categories, reporting timeframes and reporting templates provided by the DHHS Secure One. The use of common terminology, timeframes and reports will facilitate communication, reporting and incident management.
3. The proponent for this document is now the Office of Information Services, Enterprise Architecture and Strategy Group.
4. Section 1.1, the definition of a security incident has been modified to include the definition from the DHHS incident handling guidance.
5. Section 1.2 Incident Categories and Reporting Time Criteria, has been added per item 1 above.
6. Table 1, Incident Categories, has been added per item 1 above.
7. Table 2, Incident Reporting Timeframe Criteria, has been added per item 1 above.
8. Section 1.3, Event Categories, has been added per item 1 above.
9. Section 1.4, Security Incident Response Phases, has minor word and formatting changes for clarity only.
10. Section 2, Incident Reporting Template and Procedures, has been added
11. Sections 3, 4 and 5 have been completely rewritten per item 1 above.
12. Section 6, Monthly Summary Reports, has been added per item 1 above.
13. Section 7, Security Alerts, has been added per item 1 above.
14. Appendix A, CMS Security Incidents Reporting Template, replaces the previous appendix.
15. Appendix B, Incidents Involving Personally Identifiable Information, replaces the previous appendix.

Executive Summary

The Centers for Medicare & Medicaid Services (CMS) is the Federal agency that administers Medicare, Medicaid and the State Children's Health Insurance Program (SCHIP). CMS is responsible for protecting health insurance and patient information used in the administration of CMS programs.

CMS' Information Security Program has numerous controls to reduce or eliminate risk to our computer systems and/or sensitive data. Preparation and coordination to handle security incidents, should they occur, improve the overall security posture of the enterprise by providing a systematic process of security incident management. Roles and responsibilities are identified, and escalation procedures are defined to provide an orderly approach to incident response. Incident response involves the following phases: preparation, detection, alert, triage, response (containment and eradication), recovery and follow-up. The goal of a systematic approach to handle security incidents is to resume system and business operations as soon as possible while preserving the incident's forensics information for further analysis and security process enhancements. Escalation procedures are based on incidents that may occur within the CMS business environment.

This procedure also covers CMS' roles and responsibilities in evaluating incidents for determining whether to notify affected individuals and others. Critical to this determination are the roles of the CMS Senior Core Leadership for Breach Notification and the Breach Analysis Team (BAT), which provides staff support to the Senior Core Leadership.

This *Incident Handling and Breach Analysis/Notification Procedure* covers business conducted by CMS employees and contracted personnel. Additionally, the procedure is incorporated by reference into CMS contracts and agreements, and is applicable to those entities as well, e.g., system development and maintenance contracts and the users of CMS data such as the research community.

CMS is an active participant in the Department of Health and Human Services (DHHS) Secure One program. Accordingly, this document adopts verbatim many definitions, incident categories, reporting timeframes and reporting templates provided by the DHHS Secure One. The use of common terminology, timeframes and reports will facilitate communication, reporting and incident management.

Table of Contents

1. Introduction

1.1 Definition

Security incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Security incidents 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 the data at risk of unauthorized access, use, disclosure, modification or destruction. Any of these incidents has the potential for jeopardizing the confidentiality, integrity or availability of an information system or the data being processed, stored or transmitted. A security incident is a violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices. While certain adverse events, (e.g., floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered computer-security incidents. A security incident becomes a breach when the incident involves the suspected or actual loss of personally identifiable information. A security event is an observable occurrence in a network or system, e.g., detected probes, infections prevented.

1.2 Incident Categories and Reporting Time Criteria

All CMS employees, contractors, and other business partners will utilize the following incident categories, Table 1 and reporting time criteria, Table 2, when reporting incidents to CMS. The incident categories and reporting time criteria are inherited from the DHHS Incident Handling Procedure.

Table 1: Incident Categories

Category	Name	Description
CAT 0	Exercise/Network Defense Testing	Used during state, federal, national, international exercises, and approved activity testing of internal/external network defenses or responses.
CAT 1	Unauthorized Access*	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
CAT 2	Denial of Service*	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
CAT 3	Malicious Code*	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
CAT 4	Inappropriate Usage*	A person violates acceptable computing use policies.
CAT 5	Probes and Reconnaissance Scams	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

PII	Personally Identifiable Information (PII) Exposure	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 their 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.

*Source: NIST Special Publication 800-61

Table 2: Incident Reporting Timeframe Criteria

Category	Reporting Timeframe
CAT 0	Not Applicable; this category is for CMS' internal use during exercises.
CAT 1	Within one hour of discovery/detection.
CAT 2	Within two hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Daily; within one hour of discovery/detection if widespread across agency.
CAT 4	Weekly.
CAT 5	Monthly; if system is classified, report within one hour of discovery.
CAT 6	Not Applicable; this category is for CMS' use to categorize a potential incident that is currently being investigated.
PII	Within one hour of discovery/detection.

1.3 Event Categories

CMS utilizes the following categories to report monthly to DHHS Secure One.

- *Malicious Code Prevented:* Viruses were prevented and did not cause any harm to any system;
- *Probes and Reconnaissance Scans Detected:* Probes and scans were detected and did not pose a serious threat to a critical system;
- *Inappropriate Usage*: Misuse of resources; or
- *Other*: Cannot be reported in any above category.

1.4 Security Incident Response Phases

1.4.1 Preparation Phase

The preparation phase is the process of establishing policies, processes, procedures and agreements covering the management and response to security incidents such as guidelines identifying levels and responses, auditing and logging, reporting guidelines, resolution and follow-up.

1.4.2 Alert Phase

The alert phase is the process of learning about a potential security incident, and reporting it to generate a Remedy incident ticket. This phase also involves the reporting of potential incidents to the CMS IT Service Desk, who will immediately refer this to the CMS Computer Security Incident Response Team (CSIRT). Alerts may arrive from a variety of sources including: monitoring of firewalls and intrusion detection systems, anti-virus software, threats received via e-mail, and media reports about new threats. The CMS CSIRT may also directly generate Remedy tickets while managing potential incidents.

1.4.3 Triage Phase

The triage phase involves the process of examining the information available about the situation to determine whether or not a security incident has occurred. During this phase, the incident component lead is assigned. If an incident has occurred, the nature of the incident is determined, the initial priority level is assigned and the documentation of all actions taken is initiated. This phase may also involve creating an Incident Response Team (IRT) to work on activities relating to incident handling. A decision to "pursue" or "protect" is made during his phase according to the sensitivity of the data and criticality of the operational system. If a decision to "pursue" is made, it assumes the intrusion or misuse continues as analyst(s) gather information about the malicious activity before proceeding to "protect" the system and initiate actions to discontinue the unauthorized actions as in the containment and eradication phases. In either case, protective actions will be performed on the system to safeguard data and system resources on the affected system. For higher priority level incidents, consideration is given to potential legal or public relations impacts arising from each course of action.

1.4.4 Response (Containment and Eradication) Phase

The response phase is the process of limiting the scope and magnitude of an incident in order to keep the incident from getting worse. Consideration is given to factors such as system backup, the risk of continuing operations, and changing passwords or access controls lists on the compromised systems and data. This phase also involves determining the cause of the incident, improving system defenses, determining system vulnerabilities and removing the cause of the incident to eliminate possibility of recurrence. It may be necessary to activate Business continuity plans. The Business Owner of the Incident Handling Coordination and Management (IHCM) Team, defined in Section 3.7, would make this determination.

1.4.5 Recovery Phase

The system and business process returns to full and normal operations during this phase. Actions include restoring and validating the system, deciding when to restore operations and monitoring systems to verify normal operations without further system or data compromise.

1.4.6 Follow-up Phase

This phase involves developing an incident report and disseminating it to appropriate entities according to established policies; identifying lessons learned from the incident handling process including the successful and unsuccessful actions taken in response to an incident; and developing recommendations to prevent future incidents and to improve enterprise security implementation.

2. Incident Reporting Template and Procedures

2.1 Template and Procedures for Non-PII Incidents

CMS information and information system security related incidents shall be reported using the template and procedures provided at Appendix A. This template and procedures apply to all incidents except for those that involve Personally Identifiable Information (PII).

2.2 Template and Procedures for PII Incidents

Incidents that concern PII shall be reported using the template and procedures set forth in Appendix B.

3. Roles and Responsibilities

The roles and responsibilities that follow are intended to be advisory and illustrative of possible incident handling and reporting. Owners of CMS systems and business functions, including their contract officers, contract specialists, project owners, government task leads and subordinate managers have a primary responsibility to be aware of and implement these procedures in their areas, particularly with respect to timely and accurate reporting in accordance with Appendix A and Appendix B. Once reported, entities like the Senior Core Leadership for Breach Notification, the Breach Analysis Team (BAT), the IHCM Team or an IRT may be engaged or activated to direct the management of the incident through the incident response phases.

3.1 System User

3.1.1 Description

CMS employees or contractor staff conducting CMS business functions.

3.1.2 Responsibilities

- Reports security incidents to the appropriate point of contact (POC) i.e., CMS IT Service Desk, Business Owner or System Technical Support as directed by the business organization.
- Works with CMS IT Service Desk, Business Owner or System Technical Support in information gathering and incident determination activities.

3.2 CMS IT Service Desk

3.2.1 Description

CMS or contractor staff which acts as the first POC for reported operational problems and security incidents.

3.2.2 Responsibilities

- Acts as the first POC for security incidents or anomalies, and records information provided by the System User, Business Owner or System Technical Support, depending on alert source.
- Generates a Remedy ticket to document the incident for CMS records.
- Immediately refers security incident to the CSIRT.

3.3 CMS Computer Security Incident Response Team (CSIRT)

3.3.1 Description

CMS contractor staff which acts as the focal point for reporting, monitoring and tracking to closure of reported operational problems and security incidents.

3.3.2 Responsibilities

- Generates alert to DHHS Secure One and issues Appendix A or B, as appropriate to the System User, Business Owner or System Technical Support to complete. Copies CMS Chief Information Officer (CIO), Chief Information Security Officer (CISO) and the System Technical Support and/or Business Owner on all alerts sent to Secure One. The CMS Senior Official for Privacy and the Beneficiary Confidentiality Board (BCB) staff are copied only on alerts involving suspected or actual compromise of personally identifiable information.
- Provides ad hoc and periodic reports on security incidents and handling of advisories to the CIO, CISO or the CMS Senior Privacy Official.
- Executes responsibilities of System Technical Support and/or Business Owner for selected incidents as requested by the Director, Enterprise Data Center Group (EDCG).

3.4 System Technical Support

3.4.1 Description

System Technical Support may be appointed by a Business Owner of a system, or a system developer/maintainer as a lead POC for incident handling and response. Individuals assigned as the System Technical Support may include system administrators, system maintainers, security staff for the General Support System or Major Application(s) affected by the security incident, Component Information System Security Officer (ISSO), or External Business Partner contact. Staff may be a combination of CMS and contractor personnel operating/maintaining the affected system(s). System Technical Support may also be managers and supervisors of CMS systems or business functions, i.e., the Business Owner, who retains this responsibility versus delegating it.

3.4.2 Responsibilities

- Report the incident to the CMS IT Service Desk if not already reported.
- Serves as the system’s or function’s focal point for security incidents for triage, response and recovery phases.
- Prepares component-level plans and procedures to address security incidents, in accordance with this document, and information security standard operating procedures.

- Contacts CMS IT Service Desk to report security incident or vice versa, depending on the alert source.
- Provides technical support and advice for incident handling, impact assessment, and technical system management, including actions to be taken if circumstances are not covered by standard operating procedures.
- Coordinates evaluation and categorization of security advisories/information.
- Refers security advisories/information involving the CMS business function to the IHCM Team, if appropriate.
- Implements changes to information systems to minimize newly discovered vulnerabilities resulting from a security incident.
- Reports incident status/resolution information to DHHS Secure One, the IHCM Team, if activated, the Senior Core Leadership for Breach Notification (if applicable), the Breach Analysis Team POC (if applicable) and the CMS IT Service Desk in accordance with this document.
- Recommends updates and closings of incident and event tickets for all categories.
- Updates and transfers ticket to IHCM Team for incidents and events as appropriate.
- Assists IHCM Team and the IRT in information gathering, forensics and reporting activities.
- Initiates escalation procedures as directed; e.g., for incidents at an Enterprise Data Center, sends electronic page to the pre-determined government/contractor staff, when appropriate, for notification, investigation, analysis, countermeasures and follow-up.
- Upon the decision of the Senior Core Leadership for Breach Notification or the Administrator, implements approved Breach notification process, e.g., mailings to individuals and press releases

3.5 Business Owner

3.5.1 Description

A Business Owner is a component or individual who have primary ownership of a major CMS business function or process. Examples are Medicare contractors, Program Safeguard Contractors, Shared Systems, Quality Improvement Organizations, Survey & Certification, Medicare Advantage Contractors, Medicare Call Centers, Enterprise Data Centers, and organizations conducting CMS sponsored research. Business Owners are key to the handling of CMS security incidents. Either in partnership with System Technical Support or in the lead role, Business Owners direct the day-to-day handling of all incidents under guidance from the IHCM (if activated) and the Senior Core Leadership for Breach Notification (if applicable).

3.5.2 Responsibilities

- Report the incident to the CMS IT Service Desk if not already reported.
- Appoint a management and staff POC for incident handling. This may be the component ISSO or his/her manager.
- Other responsibilities parallel those of the System Technical Support, but are directed at business functions generally supported externally to CMS, e.g., functions supported by contracts, agreements or memorandums of understanding.

- Provides a management representative to the BAT and participates at the executive level in the IHCM (if activated) and the Senior Core Leadership Breach Management (if applicable).
- Upon the decision by the Senior Core Leadership or Administrator, implements approved Breach notification processes, e.g., mailings to individuals, press releases.
- Provides guidance to business partners, if needed, for reporting to the CMS IT Service Desk, e.g., a Business Owner may direct partners to submit via a Central Office or Regional Office contact before the incident is sent to the CMS IT Service Desk.
- Informs the Office of Acquisitions and Grants Management if the incident constitutes a contract violation.

3.6 Incident Response Team (IRT)

3.6.1 Description

The IRT is a logical group assembled by either the Business Owner or System Technical Support POC to handle security incidents. Team membership will vary according to the nature of the security incident, systems and applications affected by the security incident, associated components with business and technical responsibilities concerning the system affected by security incident, and the need to involve contractors providing security services/support and/or other federal agency's staff. The Business Owner or System Technical Support will determine the need for an IRT. Generally, the IRT is activated by the owner of the system or business function compromised. The Director, EDCG, may utilize the CMS CSIRT as his/her System Technical Support or and IRT to handle incidents involving general support systems for which he/she is the owner.

3.6.2 Responsibilities

Performs a variety of incident handling activities throughout the Security Incident Response phases, depending on the category level and nature of security incident.

3.7 Incident Handling Coordination and Management (IHCM) Team

3.7.1 Description

The IHCM is a multi-component team that provides support and management direction to more serious security incidents. Members may include but are not limited to the CMS Chief Information Officer (CIO); the CMS Senior Official for Privacy; the CMS Chief Financial Officer (CFO); the CMS Press Officer; the Director, External Affairs; the Director, Office of E-Health Standards and Services as well as the Owner(s) of the Business function or system compromised. The IHCM is activated by the CMS CIO who will also direct membership. Activation may be informal, e.g., by e-mail, directing a level and membership of the IHCM Team. The IHCM would not be responsible for Breach analysis or notification for beneficiaries. These functions are supported by the BAT and Senior Core Leadership for Breach Notification.

3.7.2 Responsibilities

- Leads incident handling coordination activities for incidents and assesses security incident's impact and priority.
- Correlates information across multiple components' POC and Business Owner or System Technical Support.
- Coordinates information and evidence gathering, forensics effort, and follow-up activities.
- Updates and closes incident tickets for security incidents involving successful penetrations.
- Prepares and disseminates incident updates and reports to the CIO, and other entities including DHHS Secure One, as appropriate for the security priority level.

3.8 Senior Core Leadership for Breach Notification

3.8.1 Description

This group represents CMS' executive level management, similar to HHS' PII Breach Response Team, and is comprised of: the Chief Information Officer; Senior Agency Official for Privacy; Chief Financial Officer; Office of General Counsel; Director, Office of Beneficiary Information Services; Director, Office of E-Health Standards and Services, Director, Office of External Affairs; and Business Owner Component Executive. The Senior Core Leadership:

3.8.2 Responsibilities

- Oversees the risk analysis and breach notification process, including the final determination and/or recommendation of whether to notify (e.g., public notice, notification to individuals, other parties such as providers and/or other federal agencies).
- Provides a management level representative and one senior staff person to support the BAT for each executive management component (above).
- Approves BAT recommendations for individual incidents and/or obtains approval of such recommendations from the Office of the Administrator and/or Chief Operating Officer (COO).
- Approves all public notice(s) and individual notification materials.
- Keeps the Administrator and COO apprised of all significant events/activities and decisions.

3.9 Breach Analysis Team (BAT)

3.9.1 Description

The BAT is comprised of management designees and senior staff appointed by the Senior Core Leadership for Breach Notification with the exception the CIO and the Senior Official for Privacy will represent themselves in the BAT. The CMS Privacy Officer, staff from the BCB, and CMS Chief Information Security Officer are also designated members. The manager representing the Business Owner component should be at the Group Director/Deputy level. The CIO is designated as the BAT chair.

3.9.2 Responsibilities

- Analyzes the risk of identity theft or health insurance fraud in accordance with OMB requirements and Departmental guidelines. (OMB Memorandum M-07-16 provides detailed guidance including specific factors which an agency should consider in assessing the likely risk of harm caused by the breach.)
- Ensures the breach is reported to any other affected business or system owner, e.g., claims processing or program integrity for payment fraud.
- Conducts assessments of breaches in order to determine next steps, e.g., whether or not to notify, by what means (press releases, letters), and to whom (individuals, providers, other federal agencies), whether to offer credit protection services.
- Develops government cost estimates of notification and/or credit protection services.
- Drafts model breach notification letters and/or other materials in plain language, standardized to the extent possible, with specific tailoring on a case-by-case basis.
- Determines and recommends how the letter and/or public notice gets “rolled-out,” for example, by the agency, a contractor, another agency.
- Assists business owners prepare scripts for Medicare call center operations and/or frequently asked questions to post, if necessary.
- Coordinates recommendations submitted to the Senior Core Leadership for Breach Notification with the HHS PII Breach Notification Team.
- Investigates credit protection services/costs for business components.

3.10 Chief Information Officer (CIO)

3.10.1 Description

The CIO is responsible for the overall implementation and administration of the CMS Information Security Program.

3.10.2 Responsibilities

- Provides overall incident handling direction for higher priority level security incidents.
- May authorize formation of an IHCM Team and appoint a lead component (usually the Owner of the Business function or system that is compromised).
- Provides guidance for decision-making activities for security incidents escalating beyond CMS boundaries and established policies.
- Participates as a member of the Senior Core Leadership for Breach Notification.
- Chairs the BAT and provides staff support as needed.

3.11 CMS Senior Official for Privacy

3.11.1 Description

The Senior Official for Privacy is the individual designated with CMS to protect the information privacy rights of CMS employees and beneficiaries of Agency programs, and to ensure CMS has effective information privacy management processes to accomplish this important function.

3.11.2 Responsibilities

- Provides overall direction to the BAT for incidents involving compromise of individually identifiable information.
- Participates as a member of the Senior Core Leadership for Breach Notification and the BAT.
- Provides BCB staff to support on-going BAT roles and responsibilities.

3.12 CMS Chief Information Security Officer (CISO)

3.12.1 Description

The CISO assists the CIO in the implementation and administration of the CMS Information Security Program.

3.12.2 Responsibilities

- Assists the CIO in the fulfillment of his/her incident handling responsibilities.
- Maintains coordination and communication with the DHHS CISO and DHHS Security One for incident reporting, tracking and closure.
- Provides overall incident handling direction for lower priority level incidents to System Technical Support or Business Owners, and recommendations to the IHCM for more serious incidents.
- Recommends to the CIO, Senior Privacy Official, and BAT staff to activate the BAT, if not already activated, to provide advice to the Senior Core Leadership for Breach Management on breech notification.
- Participates as a member of the BAT for incidents involving system attacks and/or penetration in which PII might be compromised.
- Serves as an ad hoc consultant of the BAT for other incidents, e.g., lost laptops, stolen hard drives, missing cartridges.
- Monitors recommendations from the BAT to the Senior Core Leadership for Breach Management, as well as updates to the HHS Secure One/PII Breach Response Team.

3.13 Managed Security Services Provider (MSSP)

3.13.1 Description

Contractor staff composed of system engineers and subject matter experts that specialize in intrusion detection systems monitoring and management, firewall management, network and operating system security, malicious incident analysis and handling, and forensics analysis.

3.13.2 Responsibilities

- Monitors 24x7 Intrusion Detection System (IDS) data collected from MSSP-supplied IDS sensors.
- Generates alerts and warnings for possible security incidents, as CMS' IDS managers.
- Provides security advisories to CMS as security incident prevention mechanism.

- Supports information gathering, analysis and forensics activities during the incident handling process.
- Provides technical advice and support in areas of expertise, remotely or on-site.

3.14 Other Entities

3.14.1 Description

CMS Executive Leadership, DHHS Secure One, the Office of Inspector General's Computer Crime Unit and the United States Computer Emergency Readiness Team US-CERT).

3.14.2 Responsibilities

Provides DHHS and/or CMS with high-level direction and policies, and assistance for security incident response process.

4. Security Incident Information Guidelines

Actions taken during the incident response phases vary according to the category of incident. This section describes general guidelines for incident response phases for each incident security level category.

4.1 Documentation

During the incident response phases, all analysts and administrators must keep a log of all actions taken to aid in incident handling, decision-making and reporting processes. The types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- The entity or people the component has contacted or who have contacted the component.
- Names of systems, programs, or networks affected by the incident.
- Impact analysis.

The Business Owner or System Technical Support shall maintain a chronology of the significant activities.

All documentation must be provided to the CMS IT Service Desk and the DHHS Secure One upon a recommendation for closure of the incident.

4.2 Information Release

Release of information during incident handling phases must be on a need-to-know basis. For all categories, when other entities would be notified of the incident, information release must be authorized, in consultation with CMS management. CMS will coordinate with legal and public affairs contacts for the affected entities if appropriate. Such direction may also come from the CIO or his/her designee, the IHCM or the Senior Core Leadership for Breach Notification.

4.3 BAT Records

The BAT shall maintain a record of their recommendations, as well as summary information on the actions taken on individual incidents.

5. Escalation Procedures

During the Alert Phase, a System User, Business Owner, System Technical Support, or MSSP analyst identifies and reports an actual or suspected security incident to the CMS IT Service Desk, Business Owner or System Technical Support, as appropriate for the business organization, so that a security incident ticket is opened for tracking of the incident. During the response phases for which it leads the incident handling coordination, the Business Owner or System Technical Support may subsequently form an IRT to assist on the incident response effort, as appropriate. Team membership will vary according to the category level and the nature of the security incident.

5.1 Action Steps

- The CMS IT Service Desk records information provided by a System User, Business Owner, System Technical Support or MSSP, and opens a Remedy incident ticket. The CMS IT Service Desk immediately refers the security incident to the CMS CSIRT.
- The CMS CSIRT immediately notifies DHHS Secure One and provides the reporting person or entity with the appropriate reporting template to complete. The CIO, CISO and System Technical Support or Business Owner (as applicable), are copied on all notifications. The SMC Senior Agency Official for Privacy and BAT are copied on PII incidents.
- For security incidents, the Business Owner or System Technical Support verifies the occurrence of the reported or suspected security incident, determines the nature of the risk to CMS information or information systems or business function, and updates the incident ticket, if necessary.
- Business Owner or System Technical Support immediately notifies identified IRT contacts in accordance with the approved notification list.
- Based on the alert provided by the CMS IT Service Desk to DHHS Secure One, the CIO may activate the IHCM. The BAT is activated for PII incidents.
- For security incidents and security advisory/information, the following additional steps may apply:
  - IHCM Team gathers information from Business Owner or System Technical Support for incident reporting, and coordinates incident handling efforts if multiple systems/components are affected.
  - Business Owner or System Technical Support develops a Corrective Action Plan (CAP) to protect sensitive information and resolve system vulnerabilities. Business Owner or System Technical Support also tracks CAP and reports to IHCM Team after implementation.
  - The CSIRT and/or Business Owner or System Technical Support notifies CIO of incident occurrence and impact, and issues periodic reports to the CIO, as appropriate

- Business Owner or System Technical Support keeps the CMS IT Service Desk/CSIRT and the IHCM Team (if activated) abreast of incident handling actions/progress and updates the incident ticket, as appropriate. Ad hoc progress reports to IHCM Team are issued, as required by the situation.
- Periodic reports are issued and/or prepared for the CIO, CMS upper management and outside entities, as appropriate; e.g., DHHS Secure One.
- The Business Owner or System Technical Support documents resolution information, including tally of systems affected, and updates and closes the security incident ticket as appropriate.
- The Business Owner or System Technical Support and/or CMS IT Service Desk/CSIRT prepares and disseminates reports to the CIO and other entities, as dictated by policies and specific mandates.
- IHCM Team coordinates with Legal and Public Affairs contacts to authorize and prepare public relations statements or legal preparation of evidence, if appropriate.
- System Technical Support and/or the Business Owner implements BAT recommendations that have been approved by the Senior Core Leadership for Breach Notification.
- If a violation of the law is suspected, IHCM Team may notify the Office of Inspector General’s Computer Crime Unit and submit a report to the United States Computer Emergency Readiness Team (US CERT) with a copy to the DHHS Secure One and CISO, or have the DHHS Secure One and CISO handle these notifications.

6. Monthly Summary Reports

CMS must generate monthly reports for the DHHS Secure One. The CMS monthly report summarizes the past month’s events and incidents, and may include changes to POC information, improvement suggestions, and other incident response issues of concern to CMS. The monthly summary report collects the following information:

- Viruses prevented;
- Probes and reconnaissance scans that were determined not to be causing a threat to critical system; and
- Additional information as required for the DHHS Secure One Department-wide data correlation efforts.

CMS’ monthly report is due the fifth calendar day of each month (or the following workday) for events and incidents that occurred during the previous month. Since each incident is reported separately to the DHHS Secure One, incidents need only be included in summary totals in the monthly summary report. CMS should use the DHHS online monthly summary report located at **https://intranet.hisp.hhs.gov/hhs/public/**. Events should be categorized when reporting per the DHHS instructions.

7. Security Alerts

The following steps constitute the procedures used by the DHHS CISO to notify Operation Divisions (OPDIVs) whenever an information security alert is available.
The DHHS CISO receives an information security alert from the following sources:

- By Monitoring the GFIRST portal for notices, alerts, and inquiries from US-CERT.
- An OPDIV finding a potential threat to the department
- Another department within the government finding a potential threat

The DHHS CISO will formulate a communication clearly defining the issue, stating the risk of the threat, and providing instructions on what remedial steps need to be taken.
The DHHS CISO will then take this communication and send it to the appropriate individuals via DHHS Secure One Support. The distribution list includes points of contact throughout CMS.

Appendix A: CMS Security Incidents Reporting Template

<table>
<tr><th colspan="5">CMS Security Incident Report</th></tr>
<tr><th colspan="5">Incident Detector’s Information</th></tr>
<tr><td>Date/Time of Report</td><td colspan="4"></td></tr>
<tr><td>First Name</td><td colspan="4"></td></tr>
<tr><td>Last Name</td><td colspan="4"></td></tr>
<tr><td>OPDIV</td><td colspan="4"></td></tr>
<tr><td>Title/Position</td><td colspan="4"></td></tr>
<tr><td>Work Email Address</td><td colspan="4"></td></tr>
<tr><td>Contact Phone Numbers</td><td><i>Work</i></td><td><i>Government Mobile</i></td><td><i>Government Pager</i></td><td><i>Other</i></td></tr>
<tr><th colspan="5">Reported Incident Information</th></tr>
<tr><td>Initial Report Filed With (Name, Organization)</td><td colspan="4"></td></tr>
<tr><td>Start Date/Time</td><td colspan="4"></td></tr>
<tr><td>Incident Location</td><td colspan="4"></td></tr>
<tr><td>Incident Point of Contact (if different than above)</td><td colspan="4"></td></tr>
<tr><td>Priority</td><td colspan="4"><i>Level 1 / Level 2</i></td></tr>
<tr><td>Possible Compromise of PII?</td><td colspan="4"><i>YES / NO</i></td></tr>
<tr><td>Privacy Information</td><td colspan="4"><i>Was the incident a violation of the Privacy Act? / Did the target suffer an adverse effect? / As a result, was the OPDIV the direct or proximate cause of the adverse effect? \ Was the violation intentional or willful? / Was the PII used maliciously? / INCLUDE PRIVACY IMPACT BELOW</i></td></tr>
<tr><td>Incident Type</td><td colspan="4"><i>Exposure of information / Alteration or destruction of information / Increased notoriety of attacker / Loss of reputation of target / Theft of IT resources / Theft of other assets</i></td></tr>
<tr><td>US-CERT Category</td><td colspan="4"><i>DoS / Malicious Code / Probes and Scans / Unauthorized Access / Other</i></td></tr>
<tr><td>US-CERT Submission Number</td><td colspan="4"></td></tr>
<tr><td>Description</td><td colspan="4"></td></tr>
<tr><td>Additional Support Action Requested</td><td colspan="4"></td></tr>
<tr><td>Method Detected</td><td colspan="4"><i>IDS/Log Review/ A/V Systems/ User Notification/ Other</i></td></tr>
<tr><td>Number of Hosts Affected</td><td colspan="4"></td></tr>
<tr><td>OPDIV / Department Impact</td><td colspan="4"></td></tr>
<tr><td>Information Sharing</td><td colspan="4"><i>Entities with which CMS and US-CERT can share incident data.</i></td></tr>
<tr><td>System</td><td colspan="4"><i>Name of FISMA reported system (if known)</i></td></tr>
<tr><td>Status</td><td colspan="4"><i>Ongoing/ Resolved/ Etc.</i></td></tr>
<tr><th colspan="5">Attacking Computer(s) Information</th></tr>
<tr><td>IP Address / Range</td><td>Host Name</td><td>Operating System</td><td>Ports Targeted</td><td>System Purpose</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Victims Computer(s) Information				
IP Address / Range	**Host Name**	**Operating System**	**Ports Targeted**	**System Purpose**
Action Plan				
Action Description				
Requestor				
Assignee				
Time Frame				
Status				
Conclusion / Summary				
Entities Notified				
Resolution	*Include whether lost materials recovered as part of the solution*			

Appendix B: Incidents Involving Personally Identifiable Information (PII)

An incident has occurred that involves Personally Identifiable Information (PII). The available details of this incident are listed below. Note the checkbox indicating the status of the incident.

□ Initial Notification □ Update □Resolution

Key Information

<Incident Title – CMS (month Day, Year)>

- <One or two sentence description>
- <Describe the roles of the people involved, be it contractors, government employees, etc.>
- <Who owned the PII?>
- <The type of PII compromised>
- <Number of individuals impacted>
- <Name of FISMA reported system, if known>
- <Current Status>
- <Remedial steps taken and steps planned to be taken>

Executive Summary

<High level summary of incident elaborating on bulleted format>

Detailed Incident Description

<Detailed description of incident with time stamps>