

Appendix A: CMS Security Incidents Reporting Template

CMS Security Incident Report				
Incident Detector's Information				
Date/Time of Report				
First Name				
Last Name				
OPDIV				
Title/Position				
Work Email Address				
Contact Phone Numbers	Work	Government Mobile	Government Pager	Other
Reported Incident Information				
Initial Report Filed With (Name, Organization)				
Start Date/Time				
Incident Location				
Incident Point of Contact (if different than above)				
Priority	Level 1 / Level 2			
Possible Compromise of PII?	YES / NO			
Privacy Information	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			
Incident Type	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			
US-CERT Category	DoS / Malicious Code / Probes and Scans / Unauthorized Access / Other			
US-CERT Submission Number				
Description				
Additional Support Action Requested				
Method Detected	IDS/Log Review/ A/V Systems/ User Notification/ Other			
Number of Hosts Affected				
OPDIV / Department Impact Information	Entities with which CMS and US-CERT can share incident data.			
System	Name of FISMA reported system (if known)			
Status	Ongoing/ Resolved/ Etc.			
Attacking Computer(s) Information				
IP Address / Range	Host Name	Operating System	Ports Targeted	System Purpose

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	<i>Include whether lost materials recovered as part of the solution</i>			

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>

Appendix C: Incident Categories and Reporting Time Criteria

For security incident involving PII, organizations should report within one hour of discovery/detection:

Name	Description	Reporting Timeframe
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.	Within one hour of discovery/detection.

For security incidents that do not involve PII, organizations should report within the timeframes described below:

Name	Description	Reporting Timeframe
Unauthorized Access*	A person gains logical or physical access without permission to a network, system, application, data, or other resource.	Within one hour of discovery/detection.
Denial of Service*	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.	Within two hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
Malicious Code*	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.	Daily; within one hour of discovery/detection if widespread across agency.
Inappropriate Usage*	A person violates acceptable computing use policies.	Weekly.
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.	Monthly; if system is classified, report within one hour of discovery.
Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for CMS' use to categorize a potential incident that is currently being investigated.

*Source: NIST Special Publication 800-61