Computer Security Incident Report

Date/Time:

Incident Tracking Number		
CMS	**HHS**	**US CERT**

**** = Required information***

Reporting Individual Contact Information			
Name*		**Email***	
Office Number*	**Cell Number**	**Dept/OPDIV***	**UserID**
Name(s) of Dept/OPDIV or individual notified of security incident:			
Dept/OPDIV	**Name/Title**	**Date/Time Notified**	

Impacted User Contact Information			
Name*		**Email***	
Office Number*	**Cell Number**	**Dept/OPDIV***	**UserID**

Incident Category			
	PII | PHI | FTI Incident (Section A)		CAT 5 Scans/Probes (*Section H*)
	CAT 0 Exercise/Network Defense Testing (*Section B*)		CAT 6 Investigations (*Section I*)
	CAT 1 Unauthorized Access (*Section C*)		CAT 7 Other (*Section J*)
	CAT 2 Denial of Service (*Section D*)		CAT 8 Lost/Stolen Asset (*Section K*)
	CAT 3 Malicious Code (*Section E*)		CAT 99 Non-Incident (*Section L*)
	CAT 4 Improper Usage (*Section F*)		

Computer Security Incident Report

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

Threat Vector Identification*		
Threat Vector		**Description**
	UNKNOWN	Cause of atack is unidentified
	ATTRITION	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks or services
	WEB	An Attack executed from a website or web-based application.
	E-MAIL	An attack executed via e-mail message or attachment.
	EXTERNAL/REMOVABLE MEDIA	An attack executed from removable media or a perifpheral device.
	IMPERSONATION / SPOOFING	An attack involving replacement of legitimate content/services with a malicious substitute.
	IMPROPER USAGE	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above catagories.
	LOSS OR THEFT OF EQUIPMENT	The loss or theft of a computing device or media used by the organization.
	OTHER	An attack does not fit into any other vector.

Computer Security Incident Report

Section A: PII / PHI / FTI Breach			
Breach Category - Check Below			
	Document Theft		Improper Usage
	Hardware / Media Theft		Unintended manual Disclosure
	Document Loss		Unintended Electronic Disclosure
	Hardware / Media Loss		Hacking or IT Incident
	Document Lost in Transit		Document sent to Wrong Address
	Hardware / Media Lost in Transit		

Number and Description of PII / PHI / FTI Lost or Compromised			
List Number Below			
	Exact Number of PII:		Check Here if Number is Unknown:
Brief Description			
Include PII / PHI / FTI format (email, web, database, etc), population effected, lost/stolen, summary time stamp and actions taken.			

Section B: Exercise / Testing (CAT 0)		
Testing Point of Contact		Testing Time Period
Name:		
Phone:		
Brief Description of Test: Including reason for test and networks / systems involved		

Section C: Unauthorized Access (CAT 1)
Describe Violation
Actions Taken (If Any)

Section D: Denial of Service (CAT 2)
Describe Violation
Actions Taken (If Any)

Section E: Malicious Code (CAT 3)				
Malware Type		Malware Name (if Known)		
	Worm			
	Virus	Action Taken		
	Trojan		Quarantined	
	Buffer Overflow		Cleaned	
	Denial of Service		No Action	
	Other	Forensic Image Taken		
		Yes		No
Describe Violation				
Actions Taken (If Any)				

Section F: Improper Usage (CAT 4)	
Type of Violation	
	(P2P) File Sharing
	Instant Messenger
	Inappropriate Web Site
	Remote Access
	Unapproved Software
	Other
Describe Violation	

Section H: Scans / Probes / Attempted Access (CAT 5)		
Timeframe of Activity	Date:	Time:
Source IP / Subnet	Source Port(s)	
Destination IP / Subnet	Destination Port(s)	
Description of Activity		
Actions Taken		

Section I: Investigation (CAT 6)		
Timeframe of Activity	Date:	Time:
Detailed Description of Activity		
Actions Taken		

Section I: Other (CAT 7)		
Timeframe of Activity	Date:	Time:
Description		

Section H: Lost / Stolen Asset (CAT 8)			
Device / Media / Object Type			
	Cell Phone		PDA
	Computer (Non-Specific)		Server
	Computer Files		Tape / DLT / DASD
	Desktop Computer		USB Thumb Drive
	E-mail		Other
	Hard Drive (External)		Laptop
	hard Drive (Internal)		Paper Documents
Description			
Actions Taken			

Section I: Non-Incident (CAT 99)
Detailed Description of Activity
Actions Taken