INFORMATION SECURITY INCIDENT REPORTING FORM

INCIDENT TRACKING INFORMATION	
Reporting Incident Number:	Organization Tracking:
REPORTING INFORMATION	
Name:	Organization:
Telephone:	Email:
Fax:	Alternate Contact:
CATEGORIZATION INFORMATION	
Primary Incident Category: Select a Primary Incident Category	Secondary Incident Category: Select a Secondary Incident Category if applicable
Delivery Vector: Select a Delivery Vector	System Weaknesses:
INCIDENT STATUS	
Status: Select Status	Last Update:
Incident Start Date:	Incident End Date:
Date Reported To AF SAP CIO:	Date Reported To AF SAP CIO:
System Classification:	Action Taken:

TECHNICAL DETAILS	
Event/Incident Description:	Root Cause(s):
Technique, Tool, or Exploit Used:	Method of Detection:
Operation System (OS):	OS Version:
SITES INVOLVED	
MAJCOM: System Name/Unique ID:	Physical Location:
Detecting Organization:	Affected Organization:
IMPACT ASSESSMENT	
Number of Systems Affected:	Direct/Indirect Costs:
Operational Impact:	Technical Impact:
ADDITIONAL REPORTING/COORDINATION	
PSO Comments:	
PSO Reporting:	SAPMO Reporting:
AF SAP CIO Reporting:	DoD SAP CIO Reporting:
Intel Reporting:	Law Enforcement/Counter Intel Reporting:

Instructions for Completing Form

Field	Description
	INCIDENT TRACKING INFORMATION
Reporting Incident Number	Units will use numbers consisting of organization name, year, and sequential numbers followed by an "IR" to differentiate from documentation tracking logs (For example, UNIT-2018-001-IR)
Organization Tracking	Identify the organization responsible for tracking the incident
	REPORTING INFORMATION
Name	The first and last name of the individual reporting the incident
Organization	The name of the organization reporting the incident
Telephone	The telephone number to be used to reach the reporting entity for additional information. The number can be for an individual's number or the central number for the organization.
Email	The email address that should be used to reach the reporting entity for additional information. The email can be for an individual or central email for the organization. Please annotate NIPR for unclassified email addresses.
Fax	The fax number to be used to reach the reporting entity for additional information.
Alternate Contact	The name, telephone number, and email of an alternate contact in the event the reporter is not available.
	CATEGORIZATION INFORMATION
Primary Incident Categorization	Identify the primary underlying cause of the incident being reported IAW Attachment A (Cyber Incident and Reportable Event Categorization).
Secondary Incident Categorization	Identify any secondary causes for which the incident is being reported, if more than one category applies, IAW Attachment A (Cyber Incident and Reportable Event Categorization).
Delivery Vector	Identify delivery vector IAW Attachment B (Delivery Vectors).
System Weaknesses	List any weakness in the information system, system security procedures, internal controls, implementation/ configuration and/or JSIG security families and controls that should have been in place. For example, an incident that had a missing patch, poor baseline system configuration, and out-of-date AV signatures as its root causes may have the following IS weaknesses associated with it: (1) Configuration Management (2) System and Information Integrity
	INCIDENT STATUS
Status	Status of incident ("OPEN," "INVESTIGATING," "MITIGATED," or "CLOSED").
Incident Start Date	The date of the earliest event that was incorporated into the incident. Provide both date and time.
Incident End Date	The date of the last time the report was updated. Provide both date and time.
Last Update	The date and time of the last time the report was updated.
Date Reported	The date when the incident was first reported to DAO or AAZ. Provide both date and time.
System Classification	Report the classification of the IS under attach (i.e., Unclassified, Confidential, Secret, TS, SAR, SCI}. This field is NOT used to classify the reported incident.
Action Taken	Indicates what action has been taken in response to the incident. Include notifications and associated reports. Additionally, include whether a copy of a media was taken (image hard drives}, or logs collected and disposition of

	medium and logs. If there isn't enough space, input "See attached" and attach a word document with the information.
TECHNICAL DETAILS	
Event/Incident Description	Provide a narrative description of the incident with technical details. State the use of the targeted IS and whether it is online or offline. Indicate whether the incident is ongoing.
Root Cause(s}	Identify the IS specific cause(s} of the incident. The root cause expands upon the identified delivery vector(s} and IS weaknesses by precisely identifying the sets of conditions allowing the incident to occur.
Technique, Tool, or Exploit Used	Identify the technique, tool, or exploit used.
Method of Destruction	Description of the method of detection.
Operating System (OS} and OS Version	Record the OS and the version number of the OS where the incident occurred.
SITES INVOLVED	
MAJCOM and System Name\System Unique ID (UID)	Major Command Name and the UID.
Physical Location	Identify the base, camp, post or station affected by the intrusion and/or who owns the target system and where it resides.
Detecting Organization	The name of the reporting unit or organization.
Affected Organization	The name of the reporting affected unit or organization.
IMPACT ASSESSMENT	
Number of Systems Affected	Number of ISs affected by the incident.
Direct/Indirect Costs	Costs {both direct and indirect}, to include all actions from initial detection through investigation, response, and recovery. This should include, but is not limited to, workforce expenses, analyst time, hardware/software, travel and shipping costs, and lost productivity.
Number of Systems Affected	Number of ISs affected by the incident.
Direct/Indirect Costs	Costs {both direct and indirect}, to include all actions from initial detection through investigation, response, and recovery. This should include, but is not limited to, workforce expenses, analyst time, hardware/software, travel and shipping costs, and lost productivity.