

 <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS) INFORMATION ASSURANCE (IA) IMPLEMENTATION GUIDE</p>	IMPLEMENTATION GUIDE No. 3	
	EFFECTIVE DATE 07/19/05	REVISED DATE 02/22/12
Subject: INCIDENT REPORTING AND RESPONSE PROGRAM		

1. PURPOSE AND SCOPE.

1.1. **Purpose.** This document provides guidance for incident handling and reporting within TRICARE Management Activity (TMA) based upon policy and instructions established by the Chairman, Joint Chiefs of Staff and other Defense authorities. It outlines key player responsibilities, the general Department of Defense (DoD) incident handling process, and TMA-specific requirements. The DoD Incident Handling Program is defined in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01A, effective June 24, 2009.

1.2. **Scope.** The provisions of this guide apply to all TRICARE Management Activity Components [TMA Directorates, TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO), hereafter referred to as the TMA Component(s)]. For TRICARE Contractors, this document is policy if required by contract; otherwise, it serves as information assurance guidance. The Chief Information Officers (CIO) of the Service Medical Departments are encouraged to incorporate this document into their information assurance policies and procedures.

2. ROLES AND RESPONSIBILITIES.

2.1. Overall, TMA has the responsibility to develop and maintain a comprehensive and agile incident response program to identify, analyze, report, and respond to threats to its networks and the DoD Global Information Grid (GIG). To meet that responsibility, TMA Components must comply with the DoD Incident Handling Program responsibilities in accordance with (IAW) CJCSI 6510.01F, “Information Assurance (IA) and Support to Computer Network and Defense (CND),” February 9, 2011.

2.2. To ensure these responsibilities are observed and enacted, the following TMA roles will support this program as outlined. These roles and responsibilities will include, at a minimum:

2.2.1. The Director, TMA. The Director, TMA is responsible and accountable for defense of TMA networks. Ensures development and implementation of a TMA incident handling policy and program consistent with the DoD Incident Handling Policy and Program and applicable authoritative guidance. Ensures development and delivery of workforce training and information regarding TMA incident handling policies,

procedures, and practices. Delegates incident handling management responsibilities as appropriate.

2.2.2. The Director, OCIO/IA. Develops TMA incident handling policy and procedures. Oversees implementation of TMA's incident handling program. Coordinates internal notification and follow-on responses in the event of an incident. Oversees coordination of incident handling communications within TMA and with external organizations. Notifies the Director, TMA Privacy Office regarding the need for a baseline review. Ensures development and delivery of regular, periodic incident handling policy, procedures, and practices training for the TMA workforce.

2.2.3. The Director, TMA Privacy Office. Upon awareness of a privacy-related breach, notifies and coordinates with the Director, TMA; Director, OCIO/IA; TMA IS Manager; Law Enforcement officials, and others as required. Determines the severity level of a privacy breach based on analysis and recommendations from the Incident Response Team. Provides guidance and oversight to the Director, TMA; Director, OCIO/IA; and TMA IS Manager throughout the privacy breach notification process to ensure compliance with all privacy requirements. Ensures workforce receives regular, periodic training and updates on privacy policies and practices.

2.2.4. Computer Network Defense Service Providers (CNDSP). The Defense Information Systems Agency (DISA) and Space and Naval Warfare Systems Command (SPAWAR) are the Computer Network Defense Service Providers (CNDSPs) for TMA. Upon request by the Director, TMA; his or her designee; or the Information Owner, the CNDSP initiates a Vulnerability Assessment of the network or system on which the incident occurred. Coordinates/communicates results of all analyses, investigations, and reviews with TMA officials and USCC Office of Primary Responsibility (OPR).

2.2.5. TMA General Counsel. Provides advice and guidance to the Director, OCIO/IA; Director, TMA Privacy Office; and TMA IS Manager in the event an incident requires notification of law enforcement and/or counter-intelligence.

2.2.6. TMA Information System (IS) Manager. Maintains awareness of all current and applicable regulatory guidance and USCC issuances. Ensures incidents are properly reported to the appropriate authorities consistent with proscribed guidance and timeframes, and specifically ensures incidents are properly reported to the Authorizing Official (AO), Military Health System (MHS) Chief Information Officer (CIO), and Director, TMA. Ensures effective incident management. Reports incidents or events affecting networks directly to the CNDSP using appropriate reporting formats. Submits an initial report to the CNDSP and USCC. Reports changes in the status of events, incidents, and incident-handling actions. Reports status updates to the CNDSP and to the Director, TMA Privacy Office regarding incidents that involve Protected Health Information (PHI)/Personally Identifiable Information (PII).

2.2.7. Information Assurance Manager (IAM). Maintains awareness of all current and applicable regulatory guidance and USCC issuances. Receives and analyzes reports from individual system users of any suspicious activity or information performance. Monitors logs and sensors and receives automated alerts. Reports anomalous activity to the

Director, OCIO/IA and the TMA IS Manager in timeframes proscribed in CJCSM 6510.01A. Performs technical defense and remediation actions during and post-incident. Provides information during post-incident phase to develop lessons learned, identify gaps between processes and policies, and improve IAM response for future incident response. This function may be performed by a team within the Helpdesk activity or by a team of technicians selected by the TMA IS Manager for incident response (Incident Response Team, IRT)

2.2.8. Individual User. Achieves and maintains situational and Information Assurance awareness. Notifies authorized personnel (e.g., IAM, program manager, supervisor, etc) of any observed suspicious activity or unusual information system performance in a timely manner.

3. BACKGROUND.

3.1. System security incidents are caused both by internal policy and procedure violations and external intrusions and exploitation of information system vulnerabilities. These events can result in loss of data integrity, denial of system resources, penetration of a system's defenses either by an insider or an outsider, misuse of legitimate computer resources, or damage to information or resources.

3.2. An effective response to system security incidents requires prompt recognition of the problem and immediate mobilization of skilled staff. Documentation of procedures and clear delegation of responsibilities are pertinent to the Incident Reporting and Response program. Essential components of a computer incident response are the elimination of points of vulnerability and the application of lessons learned. Observation of these essential processes lay the foundation of an effective Incident Handling program.

3.3. The primary objectives of the TMA incident handling program are:

3.3.1. Effectively contain events and incidents and isolate systems to minimize damage or impact to TMA systems or networks.

3.3.2. Safely acquire and preserve the integrity of data required for incident analysis.

3.3.3. Ensure effective coordination and communication with other agencies and organizations through the appropriate channels.

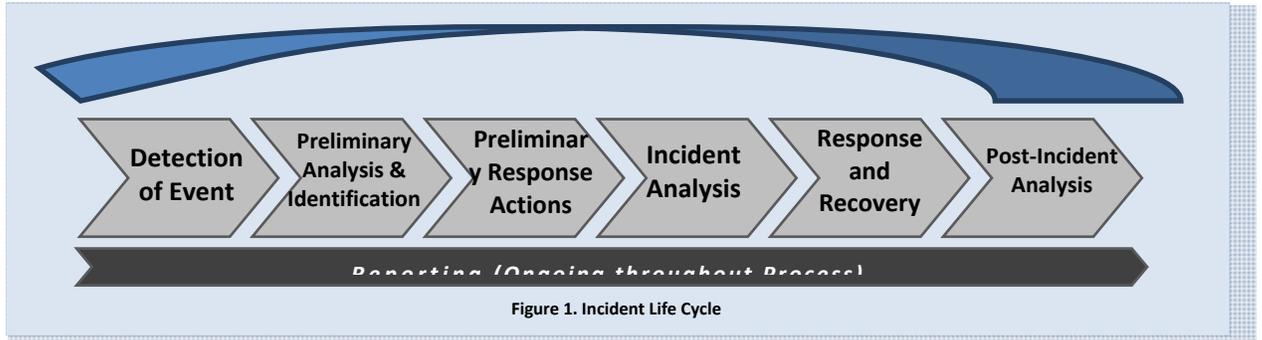
3.3.4. Provide effective and comprehensive response that includes the recovery of any affected systems and return to fully functioning, secure, operational state in a timely manner.

3.3.5. Identify lessons learned.

3.3.6. Understand patterns of activity and trends to improve our ability to identify and act in the event of a suspected incident.

4. TMA INCIDENT HANDLING GUIDANCE.

4.1. **Incident Handling and Reporting.** The life cycle for TMA incident handling aligns with the DOD incident handling lifecycle, which can be represented as diagrammed in Figure 1, below.



Note that many of these activities can happen consecutively or concurrently. Additionally, reporting should be an ongoing process throughout the incident handling lifecycle and should not be viewed as a single, specific step. High level guidance on the Incident Handling Methodology is outlined in CJCSM 6510.01A, Enclosure B.

The following table, *Relationship of Incident Handling Process and Ongoing Support Activities*, outlines the flow and coordination of steps in the incident handling process.

Relationship of Incident Handling Process and Ongoing Supporting Activities			
	Reporting and Notification	Documentation	Coordination
Detection of Events	Submission of report of events of interest	Initial documentation of event activity	Global information sharing and gathering between tiers, with other CND components, LE/CI or IC
Preliminary Analysis and Identification	Submission of initial incident report	If no documentation has been started initial documentation should occur here	Coordination to identify additional sources of information and artifacts
Preliminary Response Action	Update of actions taken	Documentation of any actions taken	Coordination of technical and organizational steps taken to implement preliminary actions across all affected C/S/As
Incident Analysis	More detailed updates of analysis performed	Documentation of analysis results	Coordination of incident analysis activities between CND and technical and management components and internal/external subject matter experts
Response and Recovery	Updates on actions taken and submission of final report for closure	Documentation of response plan, analysis performed, and COAs	Coordination of response actions between TMA IS Manager and field activities, CNDSPs, Installations and CND Service subscribers, and with LE/CI and IC, and others as required
Post-Incident Analysis	Submission of Post-Incident Analysis report	Documentation of lessons learned and resulting improvement plan	Coordination between DoD components to implement any process improvement activities resulting from post-incident analysis

Table 1. Relationship of Incident Handling Process and Ongoing Supporting Activities (CJCSM 6510.01A, Table B-1)

4.1.1. **Detection of Events.** Detection is the continuous process of identifying any unusual network or system activity, user behavior, or organizational practices and procedures with potential to adversely affect systems, networks, or operational missions. The primary objectives for detecting events include ensuring all suspicious activity is detected and reported so that further analysis can take place to determine if it is a reportable event or incident, that suspicious activity is reported in a timely manner consistent with required reporting timelines, and effectively coordinating with command channels and other DOD organizations (e.g. USCC, DISA, etc).

4.1.1.1. *Identification of Incident.* TMA components and personnel will ensure all means of identifying or detecting a possible incident will be engaged. This will include activities such as monitoring system sensors and automated alerts, receiving and assessing all end user reports of anomalous or suspicious activity on the network or of other personnel, and regularly checking USCC website message traffic.

4.1.1.1.1. End users should initially report observations to a supervisor or manager, followed by a report to the IAM. Upon becoming aware of a possible incident, the IAM will notify the activity to the Director, OCIO/IA and the TMA IS Manager. The IAM will begin the process of collecting and analyzing data to determine if there has been an incident and the extent of impact.

4.1.1.1.2. Anomalous or suspicious activity may include, but is not limited to, unusual network or device performance (e.g., sluggish, locked up), unsecure practices by other users that may put protected information at risk [e.g., transferring storage media in uncontrolled manner, using Protected Health Information (PHI)/Personally Identifiable Information (PII) in training materials, etc], or unsecured IT facilities.

4.1.1.2. If an attack is detected by USCC and reported to USCC Liaison, the Director, OCIO/IA will coordinate internal notification and follow-on responses.

4.1.2. **Preliminary Response (Analysis, Identification, and Reporting of Incidents).**

The process of conducting an initial analysis of a detected event will aid in the determination of the event as a reportable event or incident and will provide essential information required to provide reports as required by CJCSM 6510.01A. The primary objectives for this phase include determining whether a detected event is a reportable event, preventing further damage, maintaining control of the system(s) affected and the surrounding environment, collecting information in a controlled and methodical manner, and maintaining and updating the incident report and actively communicating updates through the appropriate technical and operational command channels. More detailed response steps may be taken after a more thorough analysis is performed. These will be based on the nature, scope, and potential impact of the incident.

4.1.2.1. *Incident Analysis and Identification.* Incident analysis includes a series of steps to determine if an event is a reportable event and what occurred during the incident. The TMA IS Manager coordinates with the IAM and Incident Response Team (if employed) to identify technical details, root cause(s), and potential impact of the incident, collecting the information necessary to begin forming a response or action.

4.1.2.1.1. TMA IS Manager ensures the accuracy and completeness of information compiled and provided by the IAM/Incident Response Team.

4.1.2.1.2. TMA IS Manager, in coordination with the IAM and other key players, and based on information available at a given point in the analysis, will develop an understanding of the patterns of activity that will improve TMA's ability to characterize the threat and direct protective and defensive strategies.

4.1.2.1.3. TMA IS Manager, in coordination with the IAM, systematically captures the methods used in the attack and the security controls that could prevent future occurrences.

4.1.2.1.4. The IAM/Incident Response Team researches actions that can be taken to respond to and eradicate the risk and/or threat.

4.1.2.1.5. Throughout the process, IAM/Incident Response Team specialists will work to identify the root cause(s) of the incident through technical analysis. See CJCSM 6510.01A, Enclosure D (Incident Analysis) for additional guidance.

4.1.2.2. *Initial Reporting.* Upon notification by the IAM of a possible incident, the TMA IS Manager shall ensure that incidents are properly reported to the Authorizing Official (AO); MHS Chief Information Officer (CIO); Director, TMA; and Director, OCIO/IA (if different from AO), as well as other key offices in timeframes outlined in CJCSM 6510.01A.

4.1.2.2.1. The TMA IS Manager will submit an initial report to the CNDSP and USCC. Reports will be made according to the format outlined in [Appendix D](#) to this guide. Based on TMA's reports, the CNDSP will provide reports to USCC, in turn.

4.1.2.2.1.1. *Categorization.* Reportable incidents/events must be labeled according to categories identified in [Appendix A](#).

4.1.2.2.1.1.1. Incidents in Categories 1, 2, 4, and 7 or incidents affecting Mission Assurance Category (MAC) I or II systems must be reported using Operational Report (OPREP)-3 reporting procedures IAW CJCSM 6510.01A, Enclosure C.

4.1.2.2.1.1.1.1. Root Level Intrusion (Category 1). Unauthorized privileged access to MAC I or MAC II system.

4.1.2.2.1.1.1.2. User Level Intrusion (Category 2). Unauthorized non-privileged access to MAC I or MAC II system.

4.1.2.2.1.1.1.3. Denial of Service (Category 4). Denial of Service (DoS) against MAC I or MAC II system.

4.1.2.2.1.1.1.4. Malicious Logic (Category 7). Active propagation of malware infecting a DOD IS or malicious code adversely affecting the operations and/or security of DOD IS. OPREP for previously reported outbreaks are not submitted (e.g., outbreak of virus reported two months ago).

4.1.2.2.1.2. *Reporting timelines.* Reporting timelines will be determined by category and Impact Assessment (CJCSM 6510.01A, Enclosure C - see [Appendix C](#) to this guide). Compliance with reporting timelines is required. The complete impact assessment matrix is outlined in [Appendix B](#).

4.1.2.2.1.3. *Protected Information.* If an incident involves verified Personally Identifiable Information (PII) or Protected Health Information (PHI), incidents are reported and updates are provided with sufficient detail for analysis to identify other potential threats and corrective actions to protect TMA and Department of Defense (DoD) operations. In this case, TMA IS Manager must report the incident to the United States Computer Emergency Readiness Team (US CERT) within one (1) hour (Ref. 5.2); the CNDSP and the Director, TMA Privacy Office within 1 hour (Refs. 5.2 and 5.4); and the Defense Senior Privacy Official within 24 hours (Ref. 5.2). The incident must be entered in the Joint CERT database (JCD) according to CERT requirements.

4.1.2.2.1.4. *Notification of External Agencies.* An incident may require involvement of law enforcement (LE) or counter-intelligence (CI). If the Director, OCIO/IA, in consultation with the TMA IS Manager, suspects criminal activity, especially for Categories 1, 2, 4, and 7 incidents, he or she must contact and provide reports to applicable law enforcement organizations. In rare circumstances, an incident may require reporting to counter-intelligence. Prior to taking such action, the Director, OCIO/IA and the TMA IS Manager will notify the TMA General Counsel and the Director, TMA. The Director, OCIO/IA and the TMA IS Manager will notify the CNDSP (and the Director, TMA Privacy Office when incidents involve HIPAA/PHI/PII) when they make the decision to contact law enforcement and/or counter-intelligence.

4.1.3. **Response and Recovery.** The response and recovery phase involves developing a detailed response to prevent further damage, restore integrity of the affected systems, and implement follow-up strategies to prevent recurrence of the incident. The primary focus in this phase includes resolving the incident according to policy, procedures, and quality requirements; eliminating the risk or threat; restoring the integrity of the system and returning it to an operational state; and implementing proactive and reactive

defensive and protective measures to prevent similar incidents from occurring in the future.

4.1.3.1. *Response.* Based on directions provided by USCC, CNDSP, and TMA IS Manager, as well as written CJCS, DOD, and TMA technical procedures, the IAM/Incident Response Team will perform necessary technical actions required to block access by intruders, prevent further damage to the system, and to return the affected system(s) to full operating capability.

4.1.3.2. *Recovery.* The IAM/Incident Response Team will have a readiness plan developed and prepared to be deployed during the recovery phase from an incident. TMA's recovery plan should include, at a minimum, procedures to assess and identify resulting damage to the system, identify and mitigate or prevent weaknesses in system hardware and software, review policies and procedures to ensure they meet ongoing defense requirements to deflect future attacks, communication plan and updated training plans to notify and train the TMA system owners and user community of necessary actions they must take to prevent or mitigate threats to TMA's systems and networks.

4.1.3.2.1. The nature and characterization of the incident, along with directions from USCC, the CNDSP, and guidance provided in CJCSM 6510.01A, Appendix C to Enclosure D ([Appendix B](#) to this guide) will determine the need to submit a battlefield damage assessment (BDA). Providing a BDA will improve awareness across the full spectrum of military operations to accurately characterize and understand the effects of network intrusions on the GIG and to improve military decision making about response strategies.

4.1.4. **Post-Incident Analysis.** This phase includes an after-action review of the incident, if required or directed, to evaluate the effectiveness and efficiency of TMA's incident handling for this event, and for TMA's incident handling program, overall. Information collected and developed during this phase by the IAM, TMA IS Manager, and other key players will include developing lessons learned and identifying the initial root cause, problems executing courses of action (COAs), gaps or missing policies and procedures, and inadequate infrastructure defenses.

4.1.4.1. *Outcomes.* The IAM and TMA IS Manager will use the post-incident analysis to specifically identify infrastructure problems, organizational policy and procedural problems, and technical or operational training needs. The after-action review is an instrumental part of the process that enables key managers to determine unclear or undefined roles, responsibilities, interfaces, and authority. It also serves to improve the tools available to enable the IAM to perform protection, detection, analysis, or response actions.

4.1.5. **Vulnerability Assessment.** Following a systemic event, or as a precursor to accreditation, TMA information owners affected by an incident may request a Vulnerability Assessment of its enclaves and network systems. Vulnerability Assessment, or Vulnerability Assessment Activity (VAA), is a systematic examination of an information system or product to determine the adequacy of security measures,

identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

4.1.5.1. Requests for such resources must follow TMA's chain of authority:

4.1.5.1.1. The AO will notify the Director, TMA; Director, TMA Privacy Office; and the Information Owner regarding the need for a baseline review (VAA).

4.1.5.1.2. The Director, TMA; his or her designee; or the Information Owner must formally request the CNDSP to begin a VAA.

4.1.5.1.3. The CNDSP will initiate and coordinate the VAA IAW applicable regulatory and technical guidance, providing a report to the stakeholders for review and action, as needed.

4.1.5.1.3.1. Vulnerability Assessments follow three phases:

4.1.5.1.3.1.1. Phase I – A Vulnerability Assessment Team (VAT) will examine information systems, networks, workstations, and IA policies to determine the adequacy of existing security measures and identify security deficiencies.

4.1.5.1.3.1.2. Phase II – If the VAT identifies vulnerabilities, a Blue Team (a team of knowledgeable personnel normally formed by DISA to assist in vulnerability mitigation) will provide guidance on areas of concern. The team will function as a “friendly assist” to expeditiously remedy deficiencies and enhance policy and procedures.

4.1.5.1.3.1.3. Phase III – After the VAT and Blue Team have addressed all deficiencies, a “Red Team” (a team of personnel knowledgeable in offensive attacks) conducts attacks against the TMA IT information infrastructure and attempts to discover additional weaknesses and vulnerabilities. These teams will work closely with system/network owners to demonstrate how future attacks might occur. Team leaders also will submit to system/network owners' recommendations for protecting their systems.

4.1.6. **Follow-on Reporting.** The TMA IS Manager and/or the Director, OCIO/IA will monitor after-incident operations through the IAM and report changes in the status of events, incidents, and incident-handling actions to the CNDSP and TMA leadership, including the Director, TMA; Director, TMA OCIO/IA; the Director, TMA Privacy Office and others as appropriate.

4.1.6.1. For incidents that specifically involve HIPAA/ PHI/PII, the TMA IS Manager will provide updates when:

4.1.6.1.1. There are increases, decreases, or changes in the nature of the reportable event or incident activity.

4.1.6.1.2. Corrective actions are taken that change the status of the reportable event or incident activity.

4.1.6.1.3. A reportable event or incident has been declared closed.

4.1.6.2. Updates must be reported to the CNDSP every 24 hours, until an incident is closed. The CNDSP will forward updates to the USCC. If no other directions are provided, follow-on reports are submitted within 8 hours of the discovery of new information about the incident, per CJCSM 6510.01A.

5. REFERENCES

- 1) CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND),” February 9, 2011
- 2) CJCSM 6510.01A , “Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program),” June 24, 2009
- 3) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
- 4) TRICARE Management Activity Incident Response Team and Breach Notification Policy Memorandum and Administrative Instruction Number 17, TRICARE Management Activity Incident Response Team and Breach Notification, November 5, 2009

6. ACRONYMS

AO.....Authorizing Official [previously, Designated Accrediting Authority (DAA)]
CERTComputer Emergency Response Team
CIO.....Chief Information Officer
CIRTComputer Incident Response Team
COACourse of Action
CJCSI.....Chairman of the Joint Chiefs of Staff Instruction
CJCSM.....Chairman of the Joint Chiefs of Staff Manual
CNDComputer Network Defense
CNDSP.....Computer Network Defense Service Provider
CI.....Counter-Intelligence
USCC.....United States Cyber Command
DISADefense Information Services Agency
DoD.....Department of Defense
DoDIDepartment of Defense Instruction

DTGDate Time Group

FHP&RForce Health Protection & Readiness

GIGGlobal Information Grid

HA/TMA.....Health Affairs TRICARE Management Activity

HIPAAHealth Insurance Portability and Accountability Act

IAInformation Assurance

ISInformation System

IT.....Information Technology

JCDJoint Computer Emergency Response Team (CERT) Database

JMIS.....Joint Medical Information Systems

LE.....Law Enforcement

MACMission Assurance Category

OCIO/IAOffice of the Chief Information Officer/Information Assurance

OIOperational Impact

OSOperating System

PEO.....Program Executive Office

PHIProtected Health Information

PII.....Personally Identifiable Information

TASKORD....Tasking Order

TI.....Technical Impact

TMA.....TRICARE Management Activity

TRO.....TRICARE Regional Offices

USU.....Uniformed Services University

VAA.....Vulnerability Assessment Activity (ies)

VATVulnerability Assessment Team

WAN.....Wide Area Network

APPENDIX A
INCIDENT AND REPORTABLE EVENT CATEGORIES

An Incident or Reportable Event Category is a collection of events or incidents sharing a common underlying cause for which an incident or event is reported. Each event or incident is associated with one or more categories as part of the incident handling process.

<u>Category</u>	<u>Description</u>
1	<u>Root Level Intrusion (Incident)</u> – Unauthorized privileged access to a DOD system. Privileged access, often referred to as administrative or root access, provides unrestricted access to the system. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the system is compromised with malicious code that provides remote interactive control, it will be reported in this category.
2	<u>User Level Intrusion (Incident)</u> – Unauthorized non-privileged access to a DOD system. Non-privileged access, often referred to as user-level access, provides restricted access to the system based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the system is compromised with malicious code that provides remote interactive control, it will be reported in this category.
3	<u>Unsuccessful Activity Attempt (Event)</u> – Deliberate attempts to gain unauthorized access to a DOD system that are defeated by normal defensive mechanisms. Attacker fails to gain access to the DOD system (i.e., attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.
4	<u>Denial of Service (Incident)</u> – Activity that denies, degrades or disrupts normal functionality of a system or network.
5	<u>Non-Compliance Activity (Event)</u> - Activity that potentially exposes DOD systems to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing DOD policy. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.
6	<u>Reconnaissance (Event)</u> – Activity that seeks to gather information used to characterize DOD systems, applications, networks, and users that may be useful in formulating an attack. This includes activity such as mapping DOD networks, systems devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
7	<u>Malicious Logic (Incident)</u> – Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised system. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from a DOD system.
8	<u>Investigating (Event)</u> – Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure.
9	<u>Explained Anomaly (Event)</u> – Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as system malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified.

(CJCSM 6510.01A, Table B-A-2, Incident and Reportable Event Categories)

**APPENDIX B
IMPACT ASSESSMENT MATRIX**

1. The System Impact Matrix may assist in completing an initial impact assessment when submitting a report. Initial assessment should be performed quickly even with limited details and analysis.
2. This table indicates the level of impact based on the type of device affected and the incident category. It should only be used during the initial reporting process. The more complete impact assessment conducted later in the incident handling process is done IAW CJCSM 6510.01A, Appendix C to Enclosure D (Impact Assessment Matrix), as outlined below the *Initial Impact Assessment* table.

Impact Assessment Matrix							
	Incident and Reportable Event Category						
Network Device	CAT 1	CAT 2	CAT 3	CAT 4	CAT 5	CAT 6	CAT 7
Backbone	High	High	Low	High	Low	Low	Low
Router	High	High	Low	High	Moderate	Low	Low
Network Management/ Security Server	High	High	Low	High	Moderate	Low	Moderate
Non-Public Server	Moderate	Moderate	Low	Moderate	Moderate	Low	Moderate
Public Server	Low	Low	Low	Moderate	Low	Low	Moderate
Workstation	Low	Low	Low	Moderate	Low	Low	Moderate

(CJCSM 6510.01A, Table C-B-2, Initial Impact Assessment)

1. Impact Assessment *(Extracted selected text from CJCSM 6510.01A, Appendix C to Enclosure D)*

1.1. Impact is assessed based on the degree to which an incident or event adversely affects, or has the potential to affect, the successful accomplishment of operational missions and the confidentiality, integrity, or availability of DOD systems and networks.

1.1.1. Each event or incident is assessed and assigned an impact as part of the incident handling process.

1.1.2. An impact assessment is one of the determining factors when assigning priority to an incident or event.

1.1.3. The Category and Level of Impact guide reporting timelines and response actions commensurate with the magnitude of the incident or event.

1.2. In determining the actual impact, consider the current and potential impact of the incident or event on the confidentiality, availability, and integrity of organizational operations, organizational assets, or individuals. The standards and guidelines used below to provide a baseline for assessing impact have been adopted and adapted (where necessary)

from NIST Special Publication 800-60, “Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories,” August 2008.

1.2.1. Levels of Impact

1.2.1.1. Low. The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

1.2.1.1.1. Cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.

1.2.1.1.2. Result in minor damage to organizational assets.

1.2.1.1.3. Result in minor financial loss.

1.2.1.1.4. Result in minor harm to individuals.

1.2.1.2. Moderate. The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

1.2.1.2.1. Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

1.2.1.2.2. Result in significant damage to organizational assets.

1.2.1.2.3. Result in significant financial loss.

1.2.1.2.4. Result in significant harm to individuals that do not involve loss of life or serious life threatening injuries.

1.2.1.3. High. The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

1.2.1.3.1. Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions.

1.2.1.3.2. Result in major damage to organizational assets.

1.2.1.3.3. Result in major financial loss.

1.2.1.3.4. Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

1.3. Determining Technical and Operational Impacts

1.3.1. The tables below should be used to identify the potential TI and OI of the incident or reportable event.

1.3.2. These impacts should be assessed based on the degree to which an incident or event adversely affects, or has the potential to affect, the successful accomplishment of operational missions and the confidentiality, integrity, or availability of DOD systems and networks.

1.3.3. These impacts must be recorded as part of the incident handling process and included in the incident report. For example, a DoS attack against a local MAC I/II mail server may have the following impacts:

1.3.3.1. Technical Impact

1.3.3.1.1. Confidentiality – Low.

1.3.3.1.2. Integrity – Low.

1.3.3.1.3. Availability – Medium.

1.3.3.1.4. The potential impact to technical availability is MEDIUM because it may degrade day-to-day business services.

1.3.3.2. Operational Impact

1.3.3.2.1. Confidentiality – Low.

1.3.3.2.2. Integrity – Low.

1.3.3.2.3. Availability – High.

1.3.3.2.4. The potential impact to operational availability is HIGH because it is targeted at a MAC I/II system.

APPENDIX C REPORTING TIMES

1. The Reporting Timelines outlined in CJCSM 6510.01A establish the minimum requirements and timeframes by which incidents will be reported. The table below has been revised to meet TMA OCIO directed requirements. USCC may issue changes to reporting requirements and timeframes.

2. Reporting timelines will be based on the current and potential impact of the incident or event on the confidentiality, availability, and integrity of organizational operations, organizational assets, or individuals. Follow-on reports will be submitted as directed by the higher CND organizations or headquarters. If no direction is provided, follow-on reports will be submitted within 8 hours of the discovery of new information about the incident.

3. For more information regarding the definitions for the Reporting Timelines columns, please refer to CJCSM 6510.01A, Appendix A to Enclosure C.

Category and Title	Impact	Initial Notification to CNDSP	Initial Report to CNDSP	Initial submission to JCD
1 Root Level Intrusion (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours
	Low	Within 4 hours	Within 12 hours	Within 24 hours
2 User Level Intrusion (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours
	Low	Within 4 hours	Within 12 hours	Within 24 hours
3 Unsuccessful Activity Attempt (Event)	Any	Within 4 hours	Within 12 hours	Within 24 hours
4 Denial of Service (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours
	Moderate	Within 15 minutes	Within 4 hours	Within 6 hours of discovery
	Low	Within 30 minutes	Within 6 hours	Within 8 hours
5 Non-Compliance Activity (Event)	All Non-Compliance Events	Within 4 hours	Within 12 hours	Within 48 hours
6 Reconnaissance (Event)	Any	Within 4 hours	Within 12 hours	Within 24 hours
7 Malicious Logic (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours
	Moderate	Within 2 minutes	Within 8 hours	Within 12 hours
	Low	Within 4 hours	Within 10 hours	Within 18 hours

8 Investigating (Event)	N/A	Within 2 hours of notification	Within 4 hours of notification	Within 24 hours
9 Explained Anomaly (Event)	N/A	N/A	Within 24 hours	Within 72 hours

(CJCSM 6510.01A, Table C-A-1, Reporting Timelines, revised)

APPENDIX D
INFORMATION ASSURANCE
COMPUTER INCIDENT REPORTING FORMAT

1. Use this standardized format to transmit initial and follow-on reports to the CNDSP and USCC.
2. IAW CJCSM 6510.01A, Appendix B to Enclosure C, initial reports may be incomplete; however, timely reporting is vital, and complete information should follow as details emerge. Reporting organizations should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed).

Note: *Incidents that may be classified in multiple categories will be reported at the most severe category.*

<i>CJCSM 6510.01A, Table C-B-1, General Incident Report Format, revised</i>	
Field	Description
Incident Tracking Information	
Reporting Incident Number	Identify the reporting CNDSP (e.g., CERT/CIRT) reference number for tracking the incident.
Organization Tracking	Identify the organization that is 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 or Defense Switch Network (DSN) number that should be used to reach the reporting entity for additional information. This may be the number to an individual or central number for the organization (e.g., operations center).
E-mail	The e-mail address that should be used to reach the reporting entity for additional information. This may be the e-mail address of an individual or central e-mail for the organization (e.g., operations center).
Fax	The fax number that should be used to reach the reporting entity for additional information.
Alternative Contact	The name, telephone number, and e-mail of an alternative contact in the event the reporter is not available.
Categorization Information	
Primary Incident Category	Identify the primary underlying cause of the incident being reported IAW CJCSM 6510.01A, Appendix A to Enclosure B (Incident and Reportable Event Categorization).
Secondary Incident Category	Identify any secondary causes for which the incident is being reported, if more than one category applies, IAW CJCSM 6510.01A, Appendix A to Enclosure B (Incident and Reportable Event Categorization).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Attack Vector	Identify attack vector IAW CJCSM 6510.01A, Appendix A to Enclosure D (Attack Vectors.)
System Weaknesses	Identify attack vector IAW CJCSM 6510.01A, Appendix B to Enclosure D (System Weaknesses).
Incident Status	
Status	Status of the incident (“OPEN”, “INVESTIGATING”, “MITIGATED” or “CLOSED”).
Incident Start Date	ZULU DTG of the earliest event that was incorporated into the incident. Provide year/month/day/hour/minute/seconds.
Incident End Date	ZULU DTG that incident actually ended. Provide year/month/day/hour/minute/seconds.
Last Update	ZULU date time group (DTG) of the last time the report was updated. Provide year/month/day/hour/minute/seconds.
CERT Date Reported	ZULU DTG of when the incident was first reported to the CNDSP. Provide year/month/day/hour/minute/seconds.
System Classification	Report the Classification of the system under attack (i.e., UNCLASSIFIED, CONFIDENTIAL, SECRET, TS, 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. Include whether a copy of a media was taken (image hard drives), or logs collected and disposition of mediums and logs).
Technical Details	
Event/Incident Description	Provide a narrative description of the incident with technical details. Include DTGs of significant events (start, stop, or change of activity). State the use of the targeted system and whether the system is online or offline. Indicate whether the incident is ongoing.
Root cause(s)	Identify the system specific cause(s) of the incident. The root cause expands upon the identified attack vector(s) and system weaknesses by precisely identifying the sets of conditions allowing the incident to occur.
Source IP and port	Provide source IP with resolution data identifying owner and country of source IP machine. Note: the source IP could be a DOD IP. If the intruder is known, provide all identifying information to include objective of intruder, if known. Source IP is not necessarily indicative of true origin. Footnote the source of resolution/attribution data (i.e., ARIN.org). Insert “Not Applicable” for incidents that do not involve source IP or port.
Intruder(s) (if known)	Identify the intruder or group responsible for the incident, if known.
Origin (country)	Identify the source IPs country of origin.
Target IP(s) and port	Provide target IP with resolution identifying responsible command and physical location of target IP machine (e.g., B/C/P/S, etc.). Footnote the source of resolution/attribution data (i.e., DDD NIC, nslookup, and whois). If machine is behind a NAT’ed (network address translation enabled) router or firewall then also provide the wide area network (WAN) routable address (i.e. the Internet/SIPRNET routable IP address).
Technique, tool, or exploit used	Identify the technique, tool, or exploit used.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Operating system (OS) and version of OS	Record the operating system and version number of the operating system where the incident occurred.
Use of target (e.g., Web server, file server, host)	If applicable, for what the intruder/attacker used the target system for after it was exploited, if applicable.
Technical Details	
Method of detection	Identify how the intrusion was detected (e.g., external notification, log files, network monitoring, IDS, user).
Sites Involved	
Major Command	Identify the C/S/A or field activity targeted based on owner of target IP address (e.g., USN, USAF, USSTRATCOM, and Defense Information Systems Agency (DISA)).
Combatant Command	Identify the combatant command (geographical and/or functional) targeted based on the owner of the target IP address.
Physical Location (base, camp, post, or station)	Identify the B/C/P/S affected by the intrusion and/or owns the target IP and where the physical system resides.
DOD Network	Identify network on which the incident occurred (e.g., NIPRNET or SIPRNET).
Detecting Unit or Organization	The name of reporting unit or organization.
Affected Unit or Organization	The name of reporting affected unit or organization.
Impact Assessment	
Systems Affected	Number of systems affected by the incident.
Operational Impact	Identify any detrimental effects on ability to perform mission by organization directly affected. Include organizations affected (e.g., due to being network users). Include impact on other organization(s) ability to perform mission. This includes an operational impact assessment IAW CJCSM 6510.01A Appendix C to Enclosure D (Impact Assessment Matrix).
Technical Impact	Identify any detrimental effects on the technical capabilities of the organization (e.g., data loss, service degradation, effects on other systems). This includes a technical impact assessment IAW CJCSM 6510.01A Appendix C to Enclosure D (Impact Assessment Matrix). If the technical impact cannot be determined for some reason (e.g., limited details or analysis), use CJCSM 6510.01A Table C-B-2 (Initial Impact Assessment) for a limited impact assessment.
Staff Hours Lost	This is reported as an update record and may cause the impact field to be updated. Amount of time technical support is required to identify, isolate, mitigate, resolve, and recover from the attack and repair the attacked system (do not include analyst time spent analyzing the incident).
Encompassing Cost	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, hardware/software, travel & shipping costs and lost productivity.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Additional Reporting or Coordination	
OPREP 3 Reporting	State whether the incident was reported via OPREP 3 and what headquarters received the report. Attach a copy of the OPREP 3 report to this incident report, if applicable.
Intel Reporting	State whether the incident was reported to the IC. If reported, identify the agency that was contacted and any specific actions that have been coordinated.
LE/CI Reporting	State whether the incident was reported to the LE/CI community. If reported, identify the agency that was contacted and any specific actions that have been coordinated.
Other	
Exercise Name	Name of the exercise, if applicable.
Operation Name	Name of the operation or focused operation, if applicable.

(CJCSM 6510.01A, Table C-B-1, General Incident Report Format, revised)