



TRICARE  
MANAGEMENT  
ACTIVITY

**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE  
HEALTH AFFAIRS**

SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE  
FALLS CHURCH, VIRGINIA 22041-3206

NOV 05 2009

**MEMORANDUM FOR TRICARE MANAGEMENT ACTIVITY DIRECTORS**

**SUBJECT: TRICARE Management Activity Incident Response Team and Breach Notification Policy Memorandum**

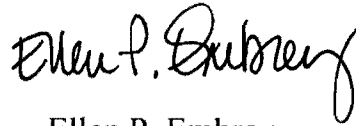
The TRICARE Management Activity (TMA) is entrusted with securing and safeguarding protected health information, personally-identifiable information, and sensitive information of our beneficiaries. As such, we are required to comply with Department of Defense (DoD) 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, and DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

In an effort to identify, mitigate, and contain the potential damage of data, this memorandum establishes a breach notification policy to institute an Incident Response Team to respond in the event of an incident. This memorandum also implements a standard process for handling and reporting breaches as defined in the attached TMA Administrative Instruction (AI) for Breach Notification. The Program Offices will be responsible for applying the requirements of the AI into their policies and procedures.

In keeping with the trust and transparency we owe our beneficiaries and as required by appropriate regulations, it is essential that all TMA workforce members report an incident. When confronted with an incident, TMA workforce members should notify their director, who should then notify the Chief Information Officer and the Privacy Officer within 1 hour of the potential or confirmed breach. Please refer to the attached TMA AI for Breach Notification or the TMA Privacy Web site located at [www.tricare.mil/tmaprivacy/dpr.cfm#incident](http://www.tricare.mil/tmaprivacy/dpr.cfm#incident).

TMA Directors shall ensure dissemination of this policy to all workforce members. For further information, please contact either the Director, TMA Privacy Office, Ms. Leslie Shaffer, who may be reached at (703) 681-7500 or

Leslie.Shaffer@tma.osd.mil; or Ms. Clarissa Reberkenny, Director, Office of the Chief Information Officer/Information Assurance, who may be reached at (703) 681-8823 or Clarissa.Reberkenny@tma .osd.mil.



Ellen P. Embrey  
Acting Director

Attachment:  
As stated

cc:  
TRICARE Regional Office/TRICARE Area Office Directors  
Office of General Counsel  
TMA Chief of Staff  
Director, Department of Defense/Veterans Affairs Program Coordination Office  
Director, Program Integration  
Defense Centers of Excellence  
Uniformed Services University of the Health Sciences

TRICARE MANAGEMENT ACTIVITY ADMINISTRATIVE INSTRUCTION  
NUMBER 17

SUBJECT TRICARE Management Activity Incident Response Team and Breach  
Notification

- References
- (a) DoD 6025.18-R “DoD Health Information Privacy Regulation,” January 24, 2003
  - (b) DoD 5400.11-R “Department of Defense Privacy Program”, May 14, 2007
  - (c) DoD 8580.02-R “DoD Health Information Security Regulation,” July 12, 2007
  - (d) “Military Health System (MHS) Information Assurance (IA) Implementation Guide No. 3, Incident Reporting and Response”, August 8, 2008
  - (e) Breach Reporting Timelines/CJCSM Reporting Timelines, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01A Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program), June 24, 2009

1. PURPOSE: This Administrative Instruction (AI)

a. Defines the process for individuals responsible for assessing an incident and handling a breach that affects TRICARE Management Activity (TMA). The Program Offices will be responsible for applying the requirements of the AI into their policies and procedures.

b. Is divided into three main sections: Roles and Responsibilities, Procedures, and Enclosures. The Roles and Responsibilities section outlines the expectations for each Program Office in the process of handling an incident. Roles may be filled by government employees, military members or contractor employees. The Procedures section details specific actions that elaborate on the roles and responsibilities.

c. Contains Appendices that provide templates, which guide the completion of various notifications and reports that are referenced throughout the procedures. Detailed descriptions of each Appendix can be found on pages 17 and 18.

## 2. APPLICABILITY AND SCOPE:

a. This AI applies to TMA Directorates, TRICARE Regional Offices (TRO), TRICARE Area Offices (TAO), and all other organizational entities in TMA (hereafter referred to as the TMA Component(s)), Defense Centers of Excellence and the Uniformed Services University of the Health Sciences.

b. This AI applies to all TMA workforce members.

c. This AI supersedes Military Health System (MHS) Standard Operating Procedure for Management of Unauthorized Disclosure of Department of Defense Sensitive Information Incidents, July 15, 2005.

## 3. DEFINITIONS:

a. Breach. The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information in which persons other than authorized users gain access or potential access to such information for other than authorized purposes in which one or more individuals will be adversely affected (Department of Defense (DoD) 5400.11-R, "DoD Privacy Program," May 14, 2007). Examples of breaches include but are not limited to unauthorized use of another user's account, unauthorized use of system privileges, extraction, or unauthorized release of DoD sensitive information (SI), and execution of malicious code that destroys DoD SI.

(1) A breach that is the result of an act that was intended to cause harm will be referred to as a malicious breach throughout the remainder of this AI.

b. Incident. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations (DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007).

c. Sensitive Information. Information in which the loss, misuse, or unauthorized access to or modification of information could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code, "The Privacy Act," but, which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Any unauthorized disclosure of SI in routine DoD payroll, finance, logistics, and personnel management systems would also be considered a breach (DoDI 8500.02, "Information Assurance (IA) Implementation," February 6, 2003).

#### 4. ROLES AND RESPONSIBILITIES:

a. The Director, TMA shall:

(1) Designate an Incident Response Team (IRT) Chairman, either the Chief Information Officer (CIO) or the Director, TMA Privacy Office, based on the nature of the breach.

(a) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Notify or assign designee to inform Health Affairs (HA).

(3) Task the following individuals to provide representatives for the IRT:

(a) Chief Information Officer (CIO)

(b) Chief of Staff (CoS)

(c) Chief Health Plan Operations (HPO)

(d) Chief Financial Officer (CFO)

(e) Chief Medical Officer (CMO), as needed

(f) Chief Force Health Protection and Readiness Programs, as needed

(g) Chief Pharmaceutical Operations, as needed

(h) Director, Program Integration (Congressional Liaison Office)

(i) Director, TMA Privacy Office

(j) Deputy Chief, Communications and Customer Service (C&CS)

(k) Director, Office of General Counsel (OGC)

(l) Director, TRICARE Procurement Support Office

(m) Director, Office of Administration

(n) Director, Defense Manpower Data Center (DMDC)

- (4) Oversee the IRT to ensure that tasks are being completed in a timely manner.
- (5) Sign or designate representative to sign breach notification letter and package.
- (6) Brief the Armed Services and Defense Appropriations Committees, as required.
- (7) Act as or assign designee to be TMA Spokesperson, and establish communication with the Services, as well as external agencies.
- (8) Ensure IRT members function in an advisory capacity for Service-level incidents involving MHS data.

b. The IRT Chairman shall:

- (1) Serve as the central point of contact (POC) for the IRT and ensure IRT members receive all information in a timely manner through meetings and e-mails.
  - (a) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.
- (2) Serve as the central POC for the Defense Manpower Data Center (DMDC).
- (3) Ensure compliance with reporting requirements (See Appendix 8), and act as the conduit of information between the Information/System Owner and the IRT.
- (4) Convene a meeting within 1 day with the IRT and ad hoc members, as required.
- (5) Ensure all IRT members have the AI for Breach Notification.
- (6) Report details of the incident to the IRT including:
  - (a) How the breach occurred.
  - (b) Dates and times when the breach was discovered.
  - (c) Current status and security of the system or business operation.
  - (d) Who has been notified.

(7) Delegate mitigation tasks to each of the IRT members and ensure completion of all tasks in a timely manner.

(8) Determine the incident severity level based on the analysis and recommendations of the IRT.

(9) Update senior leadership and the IRT as new information becomes available.

(a) For the purpose of this AI, senior leadership includes: Director, TMA; Deputy Director, TMA; Chief Health Plan Operations; Chief Information Officer; Chief Medical Officer; Chief Pharmaceutical Operations; Chief Financial Officer; Director, TRICARE Business Operations; Deputy Chief TRICARE Business Operations; Director, Privacy Office; Director, Program Integration; Director, Information Assurance; Director, Network Operations; Director, Clinical and Program Policy; Director, Communications and Customer Service; General Counsel; Deputy General Counsel; Associate General Counsel.

(10) Coordinate with the Deputy Director and CFO in estimating the costs of the breach including, but not limited to: notifying affected individuals, 1 year of free credit monitoring and identity fraud expense coverage for affected individuals, the establishment of a call center, mailings, etc.

(11) Assign responsibilities for preparation of the After Action Report for senior leadership using the standard After Action Report format (see Appendix 12).

(12) Coordinate debrief/lessons learned for Senior Leadership.

(13) Assign Action Officers (who may also be information/system owners) to create and provide to the Chairman:

(a) Summary of incident

(b) Meeting minutes

(c) Updates to senior leadership

(d) Executive Summaries

(e) Reports to external agencies, as necessary

(f) Establish a Plan of Action and Milestones (POA&M)

(g) Maintain a notebook of chronology detailing action taken, to include

executive summaries, leadership updates, e-mail communication, letters, incident reports, meeting minutes for documentation/historical purposes.

(14) Create a tracking mechanism to satisfy the general notification requirement to affected individuals.

c. The CIO Representative shall:

(1) Notify and coordinate with the IRT Chairman.

(a) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Collaborate with IRT Chairman throughout the breach process.

(3) Ensure compliance with internal incident response plan.

(4) Designate the appropriate Office of the CIO (OCIO) personnel who will report incidents affecting networks directly to the Computer Network Defense Service Provider (CNDSP). For all Category 1, 2, 4, or 7 incidents involving a Mission Assurance Category (MAC) I or II system, reports must be made to the CNDSP (Appendices 8 and 10).

(a) Report should include assets impacted, information impacted, the information owner, and actions taken to minimize vulnerabilities.

(b) Notify the TMA Office of General Counsel, TMA leadership, TMA Program Integrity, and the CNDSP prior to contacting law enforcement and/or counterintelligence agencies. In matters involving a malicious breach concerning Protected Health Information or Personally Identifiable Information TMA-PI should be TMA's liaison with law enforcement. Law enforcement notification should not be delayed.

(c) Notify the CNDSP and the TMA Privacy Office of incidents involving Protected Health Information (PHI) and Personally Identifiable Information (PII), once the decision has been made to contact law enforcement and/or counterintelligence agencies.

(d) Ensure changes in the status of events, incidents, and incident-handling actions are reported to the CNDSP when:

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



(ii) Corrective actions are taken that change the status of the reportable event or incident activity.

(iii) A reportable event or incident has been declared closed.

(5) Secure/isolate the affected equipment from the network to prevent further malicious activity.

(6) Collect information for possible forensic use including logs, inventory of systems, and personal accounts.

(7) Receive reports of possible vulnerabilities in centrally managed systems and implement the mitigation strategy.

(8) Oversee mitigation of any suspected vulnerabilities in centrally managed systems.

(9) Designate the appropriate personnel who will ensure that the incident is reported to:

(a) The Designated Accrediting Authority (DAA), the CIO, and the Director, TMA.

(b) CNDSP when the incident involves a TMA network.

(10) An incident may need the involvement of law enforcement. If the Director, Information Assurance Division (IA), in consultation with the Director, Network Operations Division, suspects criminal activity, he or she must contact applicable law enforcement organizations. In rare circumstances, an incident requires reporting to counterintelligence. Prior to taking such action, the Director, Information Assurance Division will notify the CIO, TMA General Counsel, and the Director or Deputy Director, TMA. The Director, Network Operations Division will notify the CNDSP when the decision is made to contact law enforcement and/or counterintelligence.

(a) In matters involving a malicious breach concerning PHI or PII, TMA Program Integrity should serve as TMA's liaison with law enforcement.

d. The Director, TMA Privacy Office shall:

(1) Notify and coordinate with the IRT Chairman.

(a) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(b) Determine the severity level of a breach based on analysis and recommendations from the IRT.

(c) Provide guidance and oversight to the IRT Chairman throughout the breach notification process to ensure compliance with all privacy requirements such as: incident reports, updates to leadership, and other internal and external communications.

(d) Ensure compliance with internal incident response plan.

(e) Conduct training for IRT representatives at least annually.

e. The Director, Program Integration (Congressional Liaison Office) Representative shall:

(1) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Develop, review, coordinate, and forward correspondence to the Armed Services and Defense Appropriations Committees.

(3) Provide incident response liaison services among TMA, MHS, and Congressional offices.

f. The Chief, HPO Representative shall:

(1) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Ensure the managed care, dental, and other contractors have appropriate requirements for how to handle information breaches occurring within their systems.

(3) Coordinate required acquisition actions.

g. The Deputy Chief, Communications and Customer Service (C&CS) Representative shall:

(1) Coordinate with DoD/HA Public Affairs Office (PAO) regarding any and all communications.

(a) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Draft communication plan for all target audiences including media, beneficiaries, and others for implementation by agency or organization responsible for data loss or compromise.

(3) Provide guidance and oversight for implementation of communication plan.

(4) Coordinate and review all communication products.

(5) Act as the TMA spokesperson and respond to all media queries specific to TMA actions and responsibilities. Delegates responsibilities to subject matter expert as appropriate.

(6) Provide information and guidance to all TMA Customer Service representatives within the MHS and to contractor partners to ensure they respond appropriately to beneficiary questions.

(7) Post appropriate information on TRICARE and HA Web sites.

(8) Apprise HA Communications and the Office of the Secretary of Defense (OSD) Public Affairs of communication activities.

(9) Develop comprehensive communication plans to address different levels of security breaches. These plans will be used by the agency or organization responsible for loss or data compromise.

h. The Director, Office of General Counsel (OGC) Representative shall:

(1) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Consult on legal issues including determining what qualifies as DoD SI.

(3) Provide legal advice for implementation of the DoD policy that requires notification of individuals when personal information is lost, stolen, or compromised and when the 10-day notification time period begins.

(4) Provide information to the IRT Chairman, when required.

i. The Director, TRICARE Procurement Support Office Representative shall:

(1) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Receive incident reports involving contractors.

(3) Evaluate contract language.

(4) Determine violation of contract.

j. The Director, Office of Administration Representative shall:

(1) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Receive and gather official statements and supporting documentation from all parties involved in the breach incident. A thorough inquiry will be conducted detailing all activities of the breach (i.e., who, what, when, where, how, and results).”

(3) Secure the physical location of the incident if applicable. The Security Officers at the TMA satellite offices shall secure the physical location of the breach and notify the TMA Security Manager. They shall provide a report of all activities to the TMA Security Manager.

k. The CFO Representative shall:

(1) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Assess the financial implications of the incident.

(3) Work with the Deputy Director, TMA and pertinent components to determine costs associated with damage and risk mitigation for all breaches to include: the establishment of an Incident Response Call Center, notification of affected individuals, and an offer of 1 year of free credit monitoring and identity fraud expense coverage for affected individuals, mailings, etc.

(4) Work with the Deputy Director, TMA to allocate the required resources in terms of funding to respond to the incident.

(5) Provide TMA Program Integrity support to perform liaison functions between TMA and law enforcement for malicious breaches involving PHI or PII.

1. The Information/System Owner (may also be the Action Officer) shall:

(1) Isolate the system from the rest of the network in order to preclude any further malicious activity.

(2) Define internal reporting processes, and identify a POC for the IRT.

(3) Identify compromised data including the identification of specific fields (name, rank, address, phone number, etc.).

(4) In conjunction with the CIO or Privacy Office, determine the sensitivity level of compromised data.

(5) Identify potentially affected individuals, and work through the IRT Chairman to contact DMDC for address information.

(a) Active Duty and retired members and civilians (including senior executives or flag officers) of the Army, Navy, Air Force, and Coast Guard.

(b) Contractors.

(c) Notification to all affected individuals shall be made as soon as possible, but not later than 10 working days after the breach is discovered and the identities of the individuals ascertained.

(a) Ensure first-class mail is used as the primary means of notification. However, secondary means of notification such as telephone, e-mail, and substitute notice are acceptable depending on the number of individuals affected, and what contact information is available. Additionally, when notification occurs by mail, the front of the envelope should be labeled to alert the recipient of the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the DoD Component that suffered the breach.

(6) Ensure that processes and procedures are in place for monitoring and creating an audit trail for attempts to subvert security controls for information systems and networks.

(7) Ensure mitigation tasks are executed in accordance with IRT Chairman delegation.

(8) Serve as the central POC to receive notification of security incidents for his/her system.

(9) Notify leadership of the incident upon immediate discovery that a compromise of an information system has occurred, and maintain a chronological log from the point the incident is discovered.

(10) Analyze compromised assets and identify compromised data and the information owner.

(11) Analyze system reports for forensic evidence.

(12) Employ approved eradication measures. Owners of other systems on the network may be required to implement eradication steps, even if their systems have not demonstrated symptoms of compromise.

(13) Routinely monitor IS logs and activity for any further attempts to subvert the IS.

(14) Prepare information for Help Desk staff to inform or assist users.

(15) Notify users of system availability.

(16) Coordinate system restoration upon completion of forensic analysis.

(17) Provide findings to the IRT Chairman.

m. The Director, DMDC Representative shall:

(1) Appoint an alternate to act with the authority to fulfill the requirements set forth by this section of the AI.

(2) Upon immediate notification of a data breach, assign a primary POC to provide assistance to the TMA IRT, and to coordinate the DMDC's support efforts. Immediate notification is preferable to ensure timely response to the need for information offered through DMDC.

(3) Provide database research and support to identify impacted populations.

(4) Provide database research to determine if the records of the impacted population have been accessed or otherwise compromised.

(5) Upon identification of breached population, pull the current mailing addresses, e-mail addresses, and phone numbers of the affected individuals in order to support the TMA notification to the population.

(6) If requested by TMA, provide mailing support to notify the affected population. This support includes development and review of any mail products that may be used as part of the TMA IRT.

(7) Prepare, as needed, timelines and cost estimates for services and support requested by TMA for database research and mail-out services, including the processing of return mail. Return mail services include readdressing return mail or updating the Defense Enrollment Eligibility Reporting System (DEERS) with a more current address provided with the return mail.

## 5. PROCEDURES:

a. These procedures are for conducting coherent, well-managed communications (internal and external) and coordinated management and control of an incident. The procedures include the following elements:

(1) Incident identification: Correctly identifying the incident and its severity.

(2) Incident reporting: Reporting incidents to the TMA Privacy Officer, CIO, TMA Program Integrity, senior leadership and external entities.

(3) Containment: Limiting the impact of the incident.

(4) Mitigation of harmful effects: Communicating with affected individuals, investigators, and other involved entities.

(5) Eradication: Removing the cause of the incident and mitigating vulnerabilities.

(6) Recovery: Restoration of business operations to normal status.

(7) Follow-up: Lessons learned, review of policies, and process improvement.

b. The activities involved for a comprehensive incident handling process are logically organized, but during the lifecycle of an incident they may be done repetitively, in parallel, or sequentially, depending on the incident.

### c. Incident Identification

(1) Incident identification involves the examination of all available information in order to determine if an event/incident has occurred.

(2) Action Steps for the IRT:

- (a) Analyze all available information to determine if an incident has occurred.
- (b) Confirm and classify the severity of the incident.
- (c) Determine an appropriate plan of action.
- (d) Acknowledge legal issues addressed by the OGC representative.
- (e) Create an incident identification log (electronic or written) to document and record all actions that are taken once an incident has been identified.

d. Incident Reporting

(1) Incident reporting pertains to the timely dissemination of information when an incident occurs.

(a) For internal reporting, TMA workforce members must report a potential or confirmed breach. The following notification must take place:

(b) TMA personnel must notify their TMA Component Director.

(c) The TMA Component Director will notify the CIO and the TMA Privacy Officer within 1 hour. The form for reporting a breach can be found on the Privacy Office Web site at <http://www.tricare.mil/TMAPrivacy/downloads/Breach-Rpt.doc> (See Appendix 4).

(d) All incidents involving a malicious breach of PHI or PII must be reported to TMA Program Integrity.

(e) The TMA Privacy Officer and/or the CIO will notify the Deputy Director, TMA, and senior leadership.

(a) For Service-related breaches, the TMA Privacy Office will notify the respective Service POC. Should the reporting individual(s)/facility require breach-related guidance, it is their responsibility (or the responsibility of the corresponding Service POC) to contact the TMA Privacy Office with their request. The Service POC must work with the reporting individual/facility in complying with the reporting and notification requirements. The primary obligation of the TMA Privacy Office for Service-related breaches is to ensure HA/TMA Leadership is updated accordingly.



(f) The Deputy Director, TMA or designee will notify the Assistant Secretary of Defense (Health Affairs) (ASD(HA)).

(2) Reporting is coordinated by the IRT Chairman with the Components, to ensure the following:

(a) Internal and external reporting is completed in accordance to regulations.

(b) Notify individuals within the specified time period.

(c) All breaches shall be reported to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour of discovering that a breach of PII has occurred, and in accordance with the guidelines set forth at [www.us-cert.gov](http://www.us-cert.gov). (See Appendices 1, 8, and 10). Additionally, the information/system owner is responsible for breach cancellation or updating applicable changes in the US-CERT database.

(d) Other reports that may be required are: Reports to Congress, DoD leadership, ASD(HA), Under Secretary of Defense (Personnel and Readiness) (USD) (P&R)), Service medical departments, and media/press.

(3) If the OCIO/IA office, in consultation with the Network Operations Representative, suspects criminal activity, he/she must contact applicable law enforcement organizations. In rare circumstances, an incident requires reporting to counterintelligence, in accordance with regulations.

(4) In the event of a contractor breach, the information/system owner must maintain a chronological tracking log.

e. Containment

(1) Containment involves short-term actions that are immediately implemented in order to limit the scope and magnitude of an incident.

(2) Containment activities include, at a minimum, the following action steps for the IRT:

(a) Determine a course of action concerning the operational status of the compromised system, and identify the critical information and/or computing services affected by the incident.

(b) Provide periodic situational updates.

(c) Follow existing local and higher authority guidance regarding any additional incident containment requirements.

f. Mitigation of Harmful Effects

(1) The Information/System Owner shall mitigate the harmful effects of all incidents by (breaches include both electronic and paper documents):

(a) Securing the information/taking the affected system off-line as soon as possible.

(b) Applying appropriate administrative and physical safeguards/blocking all exploited ports.

(c) Notifying other Information/System Owners of the attempted breach.

(2) Contractors operating under a Business Associate Agreement (BAA) shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of PHI by the Contractor in violation of the requirements of the BAA clause. These mitigation actions will include as a minimum those listed in this AI.

(3) Action Steps for IRT:

(a) In the case in which an incident has occurred within a TMA contractor's purview, notification should be made by the contractor's senior executive with TMA leadership approval.

(b) Notify/update senior leadership of the incident.

(c) Assess the need for providing 1 year of free credit monitoring and identity fraud expense coverage for affected individuals.

g. Eradication. Entails removing the cause of an incident and mitigating vulnerabilities pertaining to the incident. All eradication activities are to be documented by the IRT and the information/system owner.

h. Recovery

(1) Recovery is the restoration of business operations to the normal condition.

(2) Action Steps for the IRT:

- (a) Follow existing local and higher authority guidance regarding incident recovery requirements.
- (b) Document recovery response actions in the Incident Identification Log.
- (c) Verify that the business operation has returned to its normal condition.
- (d) Execute the necessary changes to the network/system.
- (e) Conduct forensic analysis of the servers.
- (f) Fully restore system and data.
- (g) Notify users of system availability.
- (h) Notify users of security upgrades due to the incident.
- (i) Ensure information integrity.

i. Follow-Up

(1) Follow-up is a critical step in the incident response process and assists with the response to and prevention of future incidents.

(2) Action Steps for the IRT:

- (a) Ensure all mitigation tasks in the POA&M are completed.
- (b) Create debrief for senior leadership.
- (c) Develop a lessons learned list, including a reassessment of the security and privacy classification of information.
- (d) Amend operating procedures and policies as appropriate and disseminate to all components.
- (e) Hold a lessons learned meeting to inform senior leadership.
- (f) Share lessons learned with TMA personnel and with other DoD organizations as applicable.

(g) Provide subsequent workforce training and awareness lessons as necessary.

(h) Engage an assessment conducted by an objective third party (Inspector General or Audit Agency). The third party would assess the IA posture of the site/system/area where the weakness/incident had been discovered.

(i) Obtain Director or Deputy Director, TMA, approval to solicit external support.

(ii) Coordinate with the CFO for funding.

j. Appendices. The Appendices are provided to assist the Program Offices identified in the AI, and are detailed as follows:

(1) Appendix 1, Incident Response Checklist: Presents a comprehensive required action checklist, which serves as guide through the entire incident response process.

(2) Appendix 2, Definitions: Details terminology that is specific to the incident response process.

(3) Appendix 3, Acronyms: Clarifies acronyms used throughout the AI.

(4) Appendix 4, Guidelines for Breach Reporting: Identifies regulatory guidance, which establishes breach reporting and notification requirements. Provides a template for complete breach reporting.

(5) Appendix 5, Plan of Action and Milestones Template: Format outlines mitigation tasks and tracks progression of milestones.

(6) Appendix 6, Points of Contact: Provides breach response staff with a template that can be populated with the contact information of appropriate Program Office personnel.

(7) Appendix 7, Breach Categories: Identifies criteria for accurate breach severity level classification.

(8) Appendix 8, Breach Reporting Timelines: Categorizes required reporting timelines based on the corresponding breach severity level classification.

(9) Appendix 9, Risk Assessment Table: Classifies the levels of risk associated with specific breached data elements, and assesses the likelihood of a breach leading to harm.

(10) Appendix 10, Computer Incident Reporting Form: Identifies technical fields pertaining to the Office of the Chief Information Officer/Information Assurance (OCIO/IA) for initial and follow-up reporting.

(11) Appendix 11, Sample Notification Letter: Provides a sample notification letter for beneficiaries impacted by a data breach.

(12) Appendix 12, After Action Report Template: Provides a tool that recognizes areas that went well, and areas where improvement is needed, resulting in recommendations for the handling of future breaches.

(13) Appendix 13, House Information Paper Template: Identifies outstanding breach-related issues requiring resolution.

## 6. EFFECTIVE DATE

This AI is effective immediately.

Ellen P. Embrey  
Acting Director

Attachments:  
As stated

APPENDIX 1  
INCIDENT RESPONSE CHECKLIST

Legend: ☉ Denotes tasks in progress ✓ Denotes completed tasks
---

Date and Time of incident: \_\_\_\_\_

Location of incident: \_\_\_\_\_

Point of Contact: \_\_\_\_\_

Date TMA was notified: \_\_\_\_\_

TMA informed by: \_\_\_\_\_

Date TMA Privacy Officer/CIO was notified: \_\_\_\_\_

Notified (DoD 5400.11-R May 14, 2007):

\_\_\_\_\_ US CERT (within 1 hour)

\_\_\_\_\_ Agency Privacy Officer/Senior Representative for the Service/Senior DoD component for Privacy (within 24 hours)

\_\_\_\_\_ Defense Privacy Office and component head (within 48 hours)

\_\_\_\_\_ All affected individuals within 10 working days of discovery of the loss, theft or compromise of personal information, and the identities of the individuals have been ascertained.

\_\_\_\_\_ Law enforcement authorities, if necessary

\_\_\_\_\_ Ensured incident is reported in accordance with appropriate reporting timelines

Incident Response Team (IRT)/Assigned Action Officers

\_\_\_\_\_ Breakdown of data

- What type of information was compromised including sensitivity and specific type

APPENDIX 1  
INCIDENT RESPONSE CHECKLIST

- Identification of potentially affected individuals:
  - Active Duty and retired members and civilians (including senior executives or flag officers) of the Army, Navy, Air Force, and Coast Guard
  - Contractors

\_\_\_\_\_ Convened a meeting within one day and included all appropriate parties, including but not limited to:

__ OCIO/IA Representative	__ Information Systems Authorized Users
__ System Owners	__ TPSO Representative
__ Information Owners	__ CFO Representative
__ Congressional Liaison Office Representative	__ TMA Physical Security Manager/Officer
__ C&CS Representative	__ Uniformed Services Privacy and Security Officers
__ TMA Privacy Officer	__ Public Affairs Office Representative
__ OGC Representative	__ Program Integration Representative

\_\_\_\_\_ Determined severity level based on analysis and recommendations of the IRT.

\_\_\_\_\_ Reported investigation findings to IRT Chairman/TMA Privacy Officer or CIO (on-going)

\_\_\_\_\_ Coordinated with system network owner and investigative services in order to gain full scope of incident

\_\_\_\_\_ Reported the details of the incident to the IRT, including:

- How the breach occurred
- The dates and times when the incident was discovered
- Current status and security of the system or business

APPENDIX 1

INCIDENT RESPONSE CHECKLIST

operation

- Who has been notified

\_\_\_\_\_ Delegated each IRT member with the appropriate mitigation task

\_\_\_\_\_ Determined a course of action concerning the operational status of the compromised system, physical space, or business practice

\_\_\_\_\_ Verified that the business operation has returned to its normal condition

\_\_\_\_\_ Ensured information is collected/preserved for possible forensics use

\_\_\_\_\_ Reviewed report by third party forensics investigation

\_\_\_\_\_ Created and provided a chronology and notebook of the incident, including:

- Summary of incident
- Meeting minutes
- Updates to senior leadership
- Executive Summaries
- Reports to external agencies, as necessary
- Establish a POA&M
- Notebook of chronology of action taken, to include executive summaries, leadership updates, e-mail communication, letters, incident reports, meeting minutes for documentation/historical purposes.

\_\_\_\_\_ Ensured that IRT members received all information in a timely manner through meetings and e-mails

\_\_\_\_\_ TMA shall determine whether TMA and/or the contractor shall make the required notification

\_\_\_\_\_ Contractor obtains TMA approval of notification letters

\_\_\_\_\_ POC for DMDC to obtain the address information, e-mail address, and phone numbers of the affected individuals and ensured that these addresses are used in the mailings

\_\_\_\_\_ Ensured a call center is established to provide responses to individuals who have additional questions/concerns

\_\_\_\_\_ Ensured a Web site is developed that included:

- Frequently Asked Questions
- General notification information



APPENDIX 1

INCIDENT RESPONSE CHECKLIST

- Information concerning identity theft, along with contact information for credit bureaus

- \_\_\_\_\_ Drafted notification letter (C&CS)
- \_\_\_ Obtain approval from Incident Response Team
  - \_\_\_ Coordination into Livelink
  - \_\_\_ Director or Deputy Director, TMA, determines who signs final notification letter
- \_\_\_\_\_ Final notification letter signed
- \_\_\_\_\_ Packaged notification letters, to include all necessary enclosures and attachments mailed out
- \_\_\_\_\_ Assisted DMDC in gathering information pertaining to those individuals for whom notification letters were returned
- \_\_\_\_\_ Assisted in the development of exception reports for those individuals without address information
- \_\_\_\_\_ Ensured press releases are prepared and issued (Responsible Party – PAO)
- \_\_\_\_\_ Provided guidance regarding Chain of Custody and certification of data destruction policies for IRT Manager
- \_\_\_\_\_ Assisted the CFO in estimating the costs of the incident to include notifying the affected individuals
- Assessed financial implications of the incident
  - Developed cost data associated with damage and risk mitigation
  - Allocated required resources in terms of funding to respond to the incident
  - Assigned financial responsibility
- \_\_\_\_\_ Ensured all involved parties completed their tasks as outlined in the designated time frames
- \_\_\_\_\_ Ensured lessons learned are documented
- \_\_\_\_\_ Coordinated debrief/lessons learned for senior leadership
- \_\_\_\_\_ Developed a comprehensive final report (After Action Report)

APPENDIX 2  
DEFINITIONS

For the purpose of this SOP, the following definitions have been tailored to the TMA and its purchase care providers:

**Breach**—Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected.

**Compromise**—Type of incident where information is disclosed to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

**Electronic Protected Health Information (ePHI)**—For the purpose of this document, ePHI is referring to individually identifiable health information that is in electronic form.

**Event**—An observable occurrence within a system and/or network, or business operation that might indicate that an incident is occurring. Examples include: system crash, packet flooding within a network, series of broken locks on doors, etc.

**Incident**—The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**Incident Response Team (IRT)**—A multidisciplinary team to foster information sharing and a joint response to incidents.

**Individually Identifiable Health Information**—Information that is a subset of health information, including demographic information collected from an individual. This information must: 1) be created or received by a health care provider, a health plan, or an employer; 2) relate to the past, present, or future physical or mental health or condition of an individual; or 3) the past, present, or future payments for the provision of health care to an individual. If the information identifies the individual or that there is a reasonable basis to believe the information can be used to identify the individual, it is considered Individually Identifiable Health Information.

**Information/System Owner**—The official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an IS. The information/system owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations. The information/system owner is

## APPENDIX 2

### DEFINITIONS

also responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements.

**Information System (IS)**—An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

**Personally Identifiable Information (PII)**—Any information about an individual maintained by an agency, 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.

**Protected Health Information (PHI)**—PHI is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to: 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered PHI.

**Sensitive Information (SI)**—Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code, "The Privacy Act," but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of Title 15, United States Code, "The Computer Security Act of 1987"). Any unauthorized disclosure of Sensitive Information in routine DoD payroll, finance, logistics, and personnel management systems would also be considered a breach.

**TRICARE Management Activity (TMA)**—The mission of TMA is to manage TRICARE; manage and execute the Defense Health Program (DHP) appropriation and the DoD Unified Medical Program; support the Uniformed Services in the implementation of the TRICARE program.

APPENDIX 3

ACRONYMS

ASD (HA)	Assistant Secretary of Defense for Health Affairs
C&CS	Communications and Customer Service
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
DAA	Designated Accrediting Authority
DEERS	Defense Enrollment Eligibility Reporting System
DHP	Defense Health Program
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoD SI	Department of Defense Sensitive Information
FAQ	Frequently Asked Questions
HA	Health Affairs
HIPAA	Health Insurance Portability and Accountability Act
HIPSCC	Health Information Privacy and Security Compliance Committee
HPO	Health Plan Operations
JMISO	Joint Medical Information Systems Office
JTF-GNO	Joint Task Force Global Network Operations
IA	Information Assurance
IRT	Incident Response Team
IS	Information System
MAC	Mission Assurance Category
OCIO	Office of the Chief Information Officer
OGC	Office of General Counsel
OMB	Office of Management and Budget

APPENDIX 3

ACRONYMS

OSD .....	Office of the Under Secretary of Defense
P&R .....	Personnel and Readiness
PAO .....	Public Affairs Office
PEO.....	Program Executive Office
PHI.....	Protected Health Information
PI.....	Program Integrity
PII .....	Personally Identifiable Information
POA&M.....	Plan of Action and Milestones
POC .....	Point of Contact
SI .....	Sensitive Information
SITREP .....	Situation Report
SOP .....	Standard Operating Procedure
TAO .....	TRICARE Area Offices
TMA .....	TRICARE Management Activity
TRO .....	TRICARE Regional Offices
US .....	United States
USD .....	Under Secretary of Defense

APPENDIX 4  
GUIDELINES FOR BREACH REPORTING

TRICARE Management Activity

Guidelines for Reporting Lost, Stolen, or Compromised Personally Identifiable and/or  
Protected Health Information

Purpose:

Protecting the privacy and security of personally identifiable information (PII) and protected health information (PHI) is the responsibility of all TRICARE Management Activity (TMA) components, including TMA Directorates, TRICARE Regional Offices (TRO), TRICARE Area Offices (TAO), and all other organizational entities within TMA. All TMA components must adhere to the reporting and notification requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2007; and DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

Definition:

DoD 5400.11-R defines "lost, stolen or compromised information," otherwise termed a breach, as follows:

"Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected. Such incidents also are known as breaches."

Guidance:

This document outlines the DoD Reporting and Notification Requirements for breaches:

1. Notify your Supervisor/Director (immediately, upon discovery)
2. Notify US-CERT (within one hour) <https://forms.us-cert.gov/report/>
  - a. If breach is internal to TMA, report to TMA Privacy Office within 1 hour.
3. Notify the Agency Privacy Officer/Senior Representative for the Service/Senior Component for Privacy (within 24 hours)
  - a. If breach is external to TMA, report to TMA Privacy Office within 24 hours at PrivacyOfficerMail@tma.osd.mil or (703) 681-7500 and the Contracting Officer within 1 hour. The breach reporting form is available on the TMA Privacy Office Web site at <http://www.tricare.mil/TMAPrivacy/downloads/Breach-Rpt.doc>.

APPENDIX 4  
GUIDELINES FOR BREACH REPORTING

4. Notify the Defense Privacy Office and Component Head (within 48 hours)

5. Notify all affected individuals within 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained, if necessary (refer to OSD Memo, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” and DoD 5400.11-R C1.5 “Notification When Information is Lost, Stolen, or Compromised”)

6. Notify law enforcement authorities, if necessary

7. Notify issuing banks if government issued credit cards are involved

If PHI is involved, please refer to the DoD 6025.18-R,, “DoD Health Information Privacy Regulation,” January 2003 and DoD 8580.02-R,, “DoD Health Information Security Regulation,” July 12, 2007 for mitigation requirements.

Breaches often occur when PII or PHI is mishandled. Examples of these types of breaches may include, but are not limited to:

- Misdirected fax documents that reach anyone other than its intended recipient
- Failing to properly secure documents when mailing or transporting
- Lost or stolen removable media devices (e.g., laptops, thumb drives, CDs)
- Transmission of unsecured e-mails and unencrypted files
- Unauthorized access to computer systems
- Inappropriate disposal of documents
- Inadvertent posting on the internet

APPENDIX 4  
GUIDELINES FOR BREACH REPORTING

**Reporting of Lost, Stolen, or Compromised**  
**Personally Identifiable and/or Protected Health Information**

Today's Date:

U.S. Cert #:

- a. Component/Organization involved; Point of Contact/E-mail/Telephone #:
  
  
  
  
  
  
  
  
  
  
- b. Date of incident and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.:
  
  
  
  
  
  
  
  
  
  
- c. Brief description of incident, to include facts and circumstances surrounding the loss, theft, or compromise:
  
  
  
  
  
  
  
  
  
  
- d. Describe actions taken in response to the incident, to include whether the incident was investigated and by whom; the preliminary results of the inquiry if then known; actions taken to mitigate any harm that could result from the loss; whether the impacted individuals are being notified, and if not notified within 10 work days, that action will be initiated to notify the Deputy Secretary; \*\*what remedial actions have been, or will be, taken to prevent a similar such incident in the future, e.g., additional training conducted, new or revised guidance issued, etc.; and any other pertinent information that you believe is relevant and pertinent:

\*\*Please fill out and submit the Plan of Action and Milestone Template  
<http://www.tricare.mil/tmaprivacy/downloads/POAandMilestones.doc>

(For Official Use Only)



APPENDIX 5

PLAN OF ACTION AND MILESTONES TEMPLATE\*

<b>Task for mitigation</b>	<b>Priority (Low, Moderate, High)</b>	<b>Milestone *</b>	<b>Milestone due date</b>	<b>Status</b>	<b>Date of completion</b>	<b>Point of contact/responsibility</b>	<b>Comments</b>

**\* The TMA Privacy Office will provide guidance on the incident response documentation and report frequency requirements**

**Explanation:**

**Task for mitigation** – The action that needs to be taken to mitigate the risk of the incident occurring again. An example is: Provide refresher training for employees,

**Priority** – If the incident is a severity of 1 or 2, the priority of the task should not be less than high. Depending on circumstances, a severity level of 3, 4 or 5 can result in a priority of low, moderate or high.

**Milestone** - Specific action steps that support the completion of the task for mitigation. Multiple milestones can support the completion of a single task.

**Milestone due date** – The date the individual milestone is scheduled to be completed

**Status** – Field for those responsible for the task to track the progress of the task

**Date of completion** – The date the task or milestone has been completed

**Point of contact/responsibility** – The name of the person responsible for ensuring the completion of the milestone or task

**Comments** – Provide additional information on the task or milestone.

APPENDIX 6  
POINTS OF CONTACT TEMPLATE

<b>Role</b>	<b>POC</b>	<b>Office</b>	<b>Work Phone</b>	<b>Mobile Phone</b>	<b>E-mail</b>
Director, TMA					
CIO					
Incident Response Team (IRT) Chairman					
PEO, JMISO Representative					
Office of the Chief Information Officer Information Assurance OCIO/IA					
Director, Network Operations Division					
TMA Privacy Officer					
Director, Program Integration (Congressional Liaison) Representative					
Chief, HPOs					
Deputy Chief, C&CS Representative					
Deputy, OGC Representative					
Director, TRICARE Procurement Support Office Representative					
Director, Office of Administration Representative					

APPENDIX 6

POINT OF CONTACT TEMPLATE

CFO Representative					
Chief, TMA Security & Safety Division Representative					
Information/System Owner					

APPENDIX 7

COMPUTER NETWORK DEFENSE INCIDENTS AND EVENTS

<b>Incident Category</b>	<b>Description</b>
1	<b>Root Level Intrusion (Incident)</b> – 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	<b>User Level Intrusion (Incident)</b> – 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	<b>Unsuccessful Activity Attempt (Event)</b> – 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	<b>Denial of Service (Incident)</b> – Activity that denies, degrades or disrupts normal functionality of a system or network.
5	<b>Non-Compliance Activity (Event)</b> – 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	<b>Reconnaissance (Event)</b> – 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	<b>Malicious Logic (Incident)</b> – Installation of software designed and/or deployed by

APPENDIX 7

COMPUTER NETWORK DEFENSE INCIDENTS AND EVENTS

	adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This <b>only</b> 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.
<b>8</b>	<b>Investigating (Event)</b> – 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.
<b>9</b>	<b>Explained Anomaly/Activity (Event)</b> – 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.

APPENDIX 7

COMPUTER NETWORK DEFENSE INCIDENTS AND EVENTS

<b>PII Impact Category</b>	<b>Description</b>
<b>High</b>	The loss of confidentiality, integrity, or availability is expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets or individuals.
<b>Moderate</b>	The loss of confidentiality, integrity, or availability is expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets or individuals.
<b>Low</b>	The loss of confidentiality, integrity, or availability is expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets or individuals

APPENDIX 8

BREACH REPORTING TIMELINES

<b>CJCSM Reporting Timelines</b>					
----------------------------------	--	--	--	--	--

Category	Impact	Initial Notification to Next Tier	Initial Report to Next Tier	Initial submission to JCD	Minimum Reporting
1 Root Level Intrusion* (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours	Tier 1
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier 1
	Low	Within 4 hours	Within 12 hours	Within 24 hours	Tier 1
2 User Level Intrusion* (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours	Tier 1
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier 1
	Low	Within 4 hours	Within 12 hours	Within 24 hours	Tier 1
3 Unsuccessful Activity Attempt (Event)	Any	Within 4 hours	Within 12 hours	Within 24 hours	Tier 2
4 Denial of Service* (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours	Tier 1
	Moderate	Within 15 minutes	Within 4 hours	Within 6 hours of discovery	Tier 1
	Low	As directed by C/S/A and Field Activity Guidance	As directed by C/S/A and Field Activity Guidance	As directed by C/S/A and Field Activity Guidance	Tier 1
5 Non-Compliance Activity (Event)	All Non-Compliance Events	Within 4 hours	Within 12 hours	Within 48 hours	Tier 2
6 Reconnaissance (Event)	Any	As directed by C/S/A and Field Activity Guidance	As directed by C/S/A and Field Activity Guidance	As directed by C/S/A and Field Activity Guidance	Tier 2

APPENDIX 8  
BREACH REPORTING TIMELINES

<b>CJCSM Reporting Timelines</b>
----------------------------------

Category	Impact	Initial Notification to Next Tier	Initial Report to Next Tier	Initial Submission to JCD	Minimum Reporting
7 Malicious Logic* (Incident)	High	Within 15 minutes	Within 4 hours	Within 6 hours	Tier 1
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier 2
	Low	As directed by C/S/A and Field Activity Guidance	As directed by C/S/A and Field Activity Guidance	As directed by C/S/A and Field Activity Guidance	Tier 2
8 Investigating (Event)	N/A	Within 2 hours of notification	Consistent with the most severe possible interpretation	Within 24 hours	Tier 2
9 Explained Anomaly (Event)	N/A	N/A	Within 24 hours	Within 72 hours	Tier 2

*Note:* Table extracted from CJCSM 6510.01A, June 24, 2009



APPENDIX 8

BREACH REPORTING TIMELINES

<b>PII Reporting Timelines</b>			
<b>OPR</b>	<b>Report To</b>	<b>Initial Report</b>	<b>Requirements</b>
<b>TMA Component Director</b>	<b>US CERT</b>	<b>W/I 1 hour of discovery</b>	The U.S. Computer Emergency Readiness Team (US CERT) within one hour of discovering that a breach of personally identifiable information has occurred. Components shall establish procedures to ensure that US CERT reporting is accomplished in accordance with the guidance set forth at <a href="http://www.us-cert.gov">www.us-cert.gov</a> .
<b>TMA Component Director</b>	<b>TMA Privacy Office</b>	<b>W/I 24 hours of discovery</b>	Briefly describe the facts of the breach to include but not limited to, date, number of people affected, type of information and actions taken.
<b>TMA Privacy Office</b>	<b>Defense Privacy Office</b>	<b>W/I 48 hours of being notified</b>	Briefly describe the facts of the breach to include but not limited to, date, number of people affected, type of information and actions taken.

APPENDIX 9

RISK ASSESSMENT TABLE

**Table 1. Risk Assessment Model**

No.	Factor	Risk Determination		<p><b>Comments:</b></p> <p>All breaches of PII, whether actual or suspected, require notification to US-CERT</p> <p><b>Low:</b> <u>Low</u> and <u>moderate</u> risk/harm determinations and the decision whether notification of individuals is made, rest with the Head of the DoD Component where the breach occurred.</p> <p><b>Moderate:</b></p> <p><b>High:</b> <u>All determinations of high risk or harm require notifications</u></p>
1.	What is the nature of the data elements breached? What PII was involved?			
	a. Name only	Low		Consideration needs to be given to unique names; those where one or only a few in the population may have or those that could readily identify an individual, i.e., public figure
	b. Name plus 1 or more personal identifier (not SSN, Medical or Financial)	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual
	c. SSN	High		
	d. Name plus SSN	High		
	e. Name plus Medical or Financial data	High		
2.	Number of Individuals Affected			The number of individuals involved is a determining factor in how notifications are made, not whether they are made
3.	What is the likelihood the information is accessible and usable? What level of protection			

APPENDIX 9

RISK ASSESSMENT TABLE

No.	Factor	Risk Determination	<p><b>Low:</b></p> <p><b>Moderate:</b></p> <p><b>High:</b></p>	<p><b>Comments:</b></p> <p>All breaches of PII, whether actual or suspected, require notification to US-CERT</p> <p><u>Low</u> and <u>moderate</u> risk/harm determinations and the decision whether notification of individuals is made, rest with the Head of the DoD Component where the breach occurred.</p> <p><b><u>All determinations of high risk or harm require notifications</u></b></p>
	applied to this information?			
	a. Encryption (FIPS 140-2)	Low		
	b. Password	Moderate/High		Moderate/High determined in relationship to category of data in No. 1
	c. None	High		
4.	Likelihood the Breach May Lead to Harm	High/Moderate/ Low		Determining likelihood depends on the manner of the breach and the type(s) of data involved
5.	Ability of the Agency to Mitigate the Risk of Harm			
	a. Loss	High		Evidence exists that PII has been lost; no longer under DoD control
	b. Theft	High		Evidence shows that PII has been stolen and could possibly be used to commit ID theft?
	c. Compromise			
	(1) Compromise w/I DoD control	Low High		No evidence of malicious intent Evidence of possibility of malicious intent
	(2) Compromise beyond DoD control	High		Possibility that PII could be used with malicious intent or to commit ID theft

*DoD Components are to thoroughly document the circumstances of all breaches of PII and the decisions made relative to the factors above in reaching their decision to notify or not notify individuals*

APPENDIX 10

COMPUTER INCIDENT REPORTING FORM

Use this form to transmit initial and follow-on reports to the CNDSP and JTF-GNO.

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

<b>Field</b>	<b>Description</b>
CERT/CIRT Incident Number	Identify the reporting CERT/CIRT's reference number for tracking the incident
Primary Incident Category	Identify access level gained as per Appendix A
Secondary Incident Category	Identify any sub access level gained, if more than one category applies, as per Appendix A
Attack Vector	Identify attack vector
Weakness	Identify system weakness
Last Update	ZULU date time group (DTG) of the last time the report was updated. Provide Year/Month/Day/Hour/Minute/Seconds
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
Status	Status of the incident ("OPEN" or "CLOSED")
System Classification	Classification of the system under attack. "UNCLASSIFIED," "CONFIDENTIAL," "SECRET," "TOP SECRET"
Detecting Unit or Organization	Name of reporting Unit or Organization
Affected Unit or Organization	Name of reporting affected Unit or Organization
Action Taken	Indicates what action has been taken in response to the incident. Include notifications and associated reports; include whether a copy of a medium was taken (image hard drives), or logs collected and disposition of mediums and logs)
Organization Tracking	TRICARE Management Activity (TMA)

APPENDIX 10

COMPUTER INCIDENT REPORTING FORM

<b>Field</b>	<b>Description</b>
CERT Date Reported	ZULU DTG of when the incident was first reported to the CNDSP/JTF-GNO. Provide Year/Month/Day/Hour/Minute/Seconds
Operational Impact	Identify any detrimental effects on ability to perform mission
Major Command	TRICARE Management Activity (TMA)
System Impact	This is a subjective field, but it is critical to get a general sense of the impact on operations of an incident
Systems Affected	Number of systems affected by the incident
Staff Hours Lost	This is reported as an update record and may cause the Impact field to be updated; amount of time your technical support 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)
Exercise Name	Name of the exercise, if applicable
Event Description	Provide a detailed description of the event, including what happened, how it occurred and the current action taken to mitigate the event
Source IP and port	Provide source IP with resolution data identifying owner and country of source IP machine <ul style="list-style-type: none"><li>▪ 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)</li><li>▪ Footnote the source of resolution/attribution data – i.e., ARIN.org</li></ul>
Intruder(s) (if known)	Identify the intruder or group that is responsible for the incident, if known
Origin (country) (if known)	Identify the Source IPs country of origin

APPENDIX 10  
COMPUTER INCIDENT REPORTING FORM

<b>Field</b>	<b>Description</b>
Target IP(s) and port	<p>Provide target IP with resolution identifying responsible command and physical location of target IP machine</p> <ul style="list-style-type: none"> <li>▪ Footnote the source of resolution/attribution data – i.e., DOD NIC, NSLOOKUP, WHOIS</li> <li>▪ 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)</li> </ul>
Technical Details	<p>Provide a narrative description of the incident with technical details</p> <ul style="list-style-type: none"> <li>▪ Include DTGs of significant events (start, stop, or change of activity)</li> <li>▪ State the use of the targeted system and whether the system is on- or off-line</li> <li>▪ Indicate whether the incident is ongoing</li> </ul>
Physical Location (base, camp, post or station)	<p>Identify the facility that is affected by the intrusion and/or owns the Target IP and where the physical system resides:</p> <ul style="list-style-type: none"> <li>▪ TMA Aurora</li> <li>▪ TMA Falls Church</li> <li>▪ TRO North</li> <li>▪ TRO South</li> <li>▪ TRO West</li> </ul> <p>Provide the address for the facility</p>
Technique, tool or exploit used	<p>Identify the technique, tool, or exploit that was used to exploit the vulnerability</p>
OS and version of OS	<p>Record the operating system and version number of the operating system where the incident occurred</p>
Use of target (e.g., web server, file server, host)	<p>If applicable, for what the intruder/attacker used the target system for after it was exploited, if applicable</p>
DOD Network	<p>Identifies network on which the incident occurred:</p> <ul style="list-style-type: none"> <li>▪ NIPR</li> <li>▪ SIPR</li> </ul>

APPENDIX 10

COMPUTER INCIDENT REPORTING FORM

<b>Field</b>	<b>Description</b>
Comments	Provide any amplifying information about the incident
Synopsis	Provide an executive summary of the incident
Contact Information:	Name:
	Organization:
	Telephone:
	Fax:
	E-mail:

APPENDIX 11  
SAMPLE NOTIFICATION LETTER

Today's Date

Dear Mr. John Miller:

On January 1, 2006, a Department of Defense (DoD) laptop computer was stolen from the parked car of a DoD employee in Washington, District of Columbia., after normal duty hours, while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the \_\_\_\_\_ Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) at its Web site at [www.consumer.gov/idtheft/con\\_steps.htm](http://www.consumer.gov/idtheft/con_steps.htm). The FTC urges you to immediately place an initial fraud alert on your credit file. The fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

DoD takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you. Should you have any questions, please call \_\_\_\_\_.

Sincerely,

Signature Block



APPENDIX 12  
AFTER ACTION REPORT TEMPLATE

Summary of the Incident:

Actions Taken:

What Went Well:

- 1.
- 2.
- 3.

Areas for Improvement:

- 1.
- 2.
- 3.

Recommendations:

- 1.
- 2.

APPENDIX 13  
CONGRESSIONAL INFORMATION PAPER TEMPLATE

Title:

Status:

- 
- 

Issues to be Resolved:

- 
- 

Background:

- 
- 

Impact:

- 
- 

POC:

Name:

Title:

TRICARE Management Activity:

Address:

Phone:

E-mail: