OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

ADMINISTRATION AND
MANAGEMENT

25 SEP 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

The Department of Defense has a continuing affirmative responsibility to safeguard personally identifiable information (PII) in its possession and to prevent its theft, loss, or compromise. It is essential that all DoD personnel, to include its contractors and business partners, ensure their actions do not contribute to, nor result in, a compromise occurring if the Department is to retain the trust of those individuals on whom information is maintained.

While the DoD has adopted policies in this critical area, the Office of Management and Budget (OMB) issued guidelines in the OMB Memorandum M-07-16 dated May 22, 2007, (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf. These requirements are intended to augment, and thereby strengthen, current agency programs.

This memorandum, reissues established guidance (Attachment) for the implementation of the OMB requirements to the extent they are not presently incorporated in the current policies and procedures prescribed by DoD 5400.11-R, "DoD Privacy Program." The policies and procedures required by OMB and promulgated by this memorandum are effective immediately and are mandatory for all DoD Components. These shall be incorporated into a future revision of DoD Directive 5400.11 and DoD 5400.11-R as appropriate.

My point of contact for any questions relating to these policies, this memorandum or for any other matters relating to the Defense Privacy Program is (b)(6) Director, Defense Privacy Office, who can be contacted at (b)(6) or email at (b)(6)

Michael L. Rhodes
Acting Director

Attachment:
As stated

Policy on Safeguarding Personally Identifiable Information and Breach Notification

The Department of Defense (DoD), through the requirements provided in this attachment, hereby establishes new privacy policy for the Department. These policies are intended to strengthen existing standards for the protection of personally identifiable information while at the same time improving the decision making process relative to breach notification and reporting.

Part I. Definitions.

Current DoD Policy:

A. Personally Identifiable Information (PII), as set forth in DoD Directive 5400.11, para E2.e and DoD 5400.11-R, para DL1.14, is defined as follows:

"Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a Social Security Number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., 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, and biometric records, including any other personal information which is linked or linkable to a specified individual)."

A number of the elements included in the above definition of PII are public information subject to release under the Freedom of Information Act and DoD 5400.7-R, DoD Freedom of Information Act Program, e.g., name, civilian grade, and salary. Other elements are For Official Use Only, but are commonly shared in the work environment, e.g., name, business phone, military rank. As such, releases of these items of information, in general, do not constitute a breach. In situations where name or other unique identifier is listed alone, the context in which the name or other unique identifier is listed must be considered and a determination of the risk (or harm) must be conducted to determine if (a) a breach has occurred, and (b) whether notification is required. For example, a general support office rolodex contains personally identifiable information (name, phone number, etc.) likely would not be considered sensitive if it were breached. However, the same information in a database of patients at a clinic which treats contagious disease likely would be considered sensitive information. In situations where this personal information is linked with a name, Social Security Number and other identifiers and direct identification is possible, a determination of the risk (or harm) must be conducted to determine if notification is required. The evaluation of risk and harm in relationship to the data elements involved and their context are discussed in Appendix A and Table 1.

B. 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."

New OMB Requirements:

OMB defines a "breach" as follows:

"A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic."

OMB also stresses that "agencies should bear in mind that notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion. Adverse affect, or risk of harm, is implicitly part of the OMB concept of breach and will be maintained in the DoD definition of breach.

New DoD Policy:

DoD Components are to utilize the factors outlined in Appendix A and Table 1, or other approved methodology, to make determinations of risk of harm associated with a breach (loss, theft or compromise) of PII.

Part II. Training.

Current DoD Policy:

DoD Directive 5400.11, para 5.4.3, provides that the Secretaries of the Military Departments and the Heads of DoD Components shall:

"Conduct training, consistent with the requirements of the Privacy Act, the provisions of the DoD Directive 5400.11 and DoD 5400.11-R for personnel assigned, employed, and detailed, including contractor personnel and individuals having primary responsibility for implementing the DoD Privacy Program."

DoD 5400.11-R, Chapter 7, outlines such training requirements, to include:

Para C7.3.1 "The training shall include information regarding information privacy laws, regulations, policies and procedures governing the Department's collection, maintenance, use, or dissemination of personal information. The objective is to establish a culture of sensitivity to, and knowledge about, privacy issues involving individuals throughout the Department";

Para C7.3.3 "Include Privacy Act training in other courses of training when appropriate. Stress individual responsibility and advise individuals of their rights and responsibilities under this Regulation to ensure that it is understood that, where personally identifiable information is involved, individuals should handle and treat the information as if it was their own"; and

Para C7.4.3 "Components shall conduct training as frequently as believed necessary so that personnel who are responsible for or are in receipt of information protected by the [Privacy Act] are sensitive to the requirements of this Regulation, especially the access, use, and dissemination restrictions. Components shall give consideration to whether annual training and/or annual certification should be mandated for all or specified personnel whose duties and responsibilities require daily interaction with personally identifiable information".

New OMB Requirements:

A. OMB now requires that agencies initially train employees and managers on their privacy and security responsibilities before such personnel are authorized access to agency information and information systems.

1. Though DoD 5400.11-R para C7.3.2.1. and C7.3.2.2 currently require orientation and specialized training be conducted, it does not provide that training will be a prerequisite before an employee or manager is permitted to access DoD systems.

2. OMB Training Guidelines. OMB requires that agencies instruct their personnel on their roles and responsibilities for collecting, maintaining, and disseminating Privacy Act information; on agency rules and procedures for implementing the Privacy Act; and on penalties for failing to comply with these requirements. Training programs can be