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

26 MAY 2006

ADMINISTRATION &
MANAGEMENT

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

SUBJECT: DoD Personnel Responsibility for Safeguarding Personally Identifiable Information

There recently have been a number of incidents where personally identifying information on individuals has been lost, stolen, or compromised. The most recent is the theft of information on 26.5 million veterans where a career Department of Veterans Affairs data analyst took home electronic data in violation of Departmental policies.

These losses have prompted the Office of Management and Budget (OMB) to remind Departments and Agencies of their responsibilities under the law and policy to appropriately safeguard such information and to ensure that agency personnel are trained as to their responsibilities in this area.

OMB also has requested that agencies remind their personnel no later than June 22, 2006, of their specific responsibilities for safeguarding personally identifiable information, the rules for acquiring and using such information, and the penalties for violating these rules.

To assist you in accomplishing this goal, I am attaching a fact sheet that captures the OMB objectives. This fact sheet either can be disseminated to personnel or can be used as a basis for developing such other guidance as you may believe is warranted. Whether this fact sheet or other guidance is used, I ask that you disseminate the required information by such means as you believe will reach the widest possible audience.

Your assistance in achieving this time sensitive mandate is greatly appreciated.

My point of contact for any questions relating to this memo or for any other matters relating to the protection of personally identifiable information is Vahan Moushegian, Jr., Director, Defense Privacy Office/703.607.2943/vahan.moushegian@osd.mil.

Ralph E Newton
for Michael B. Donley
DoD Senior Privacy Official

Attachment:
As stated

OSD 08485-06

5/26/2006 2:46:16 PM

FACT SHEET

The Privacy Act of 1974 (5 U.S.C. 552a), as implemented by DoD Directive 5400.11 and DoD 5400.11-R, prescribes a framework for the collection, maintenance, use, and dissemination of information on U.S. citizens and permanent resident aliens. In general, the statutory and regulatory authority limits the collection of personal data to information that is "relevant and necessary" to accomplish an agency purpose that is mandated by statute or executive order and prohibits the dissemination of such information except with the consent of the individual about whom the information pertains or as otherwise may be authorized by one of the enumerated exceptions to the Act.

The Act, as implemented by the DoD, also requires that agencies establish adequate safeguards to ensure the security and confidentiality of the information and that rules of conduct be established for persons involved with such information.

The DoD rules of conduct, as set forth at DoDD 5400.11, Enclosure 3, are as follows:

"DoD Personnel shall:

1. Take such actions, as considered appropriate, to ensure that personal information contained in systems of records, to which they have access to or are using incident to the conduct of official business, shall be protected so that the security and confidentiality of the information is preserved.

2. Not disclose any personal information contained in any system of records, except as authorized by DoD 5400.11-R or other applicable law or regulation. Personnel willfully making such a disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties [$5,000 fine] and/or administrative sanctions.

3. Report any unauthorized disclosure of personal information from a system of records or the maintenance of any system of records that are not authorized by DoDD 5400.11 to the applicable Privacy point of contact for his or her DoD Component.

DoD system managers for each system of records shall ensure that all personnel who either have access to the system of records or who shall develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities for protecting personal information being collected and maintained under the DoD Privacy Program."

DoD personnel, as well as DoD contractors and their employees, are stewards of the information. In this fiduciary capacity, all personnel, whether military, civilian or contractor, have an affirmative responsibility to ensure that the information is collected, maintained, used, and disseminated only as authorized by law and regulation and that the information is continually safeguarded. In essence, personnel should treat and protect the information in the same manner as they would treat and protect information about themselves.