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

ADMINISTRATION AND
MANAGEMENT

JUN 15 2006

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
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: Safeguarding Personally Identifiable Information

The Department of Defense has a continuing affirmative responsibility to protect personally identifiable information in its possession because the loss, theft, or compromise of such information can have a severe adverse impact, both emotionally and economically, on the individual.

This responsibility is rooted in the Privacy Act which provides that each agency shall:

> "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained." (5 U.S.C. 552a(e)(10))

In light of the recent compromises of Government information, especially the theft of information on 26.5 million veterans, the Office of Management and Budget (OMB) has directed that Federal agencies conduct a review of their policies and procedures, and to take corrective actions as appropriate, to ensure that adequate safeguards have been adopted to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information. This review shall address all administrative, technical, and physical means used by you to control such information.

As recent losses have involved the thefts of laptop computers and associated files, your review shall include whether your current procedures and restrictions on the use and/or removal of personally identifiable information beyond DoD premises or control (e.g., TDY, telework, working at home, etc.) are adequate to protect against the possible compromise of information if it is lost or stolen.

OMB has advised that the review shall be completed in time for agencies to include the results in an agency's 2006 Federal Information Security Management Act (FISMA) Report. Though OMB has not yet released its FISMA reporting guidance for this year, OMB has directed that agencies include any identified weaknesses in your FISMA required security plans for action and milestones. However, it can be anticipated that the FISMA guidance, once released, may well impose additional reporting requirements concerning the review.

My point of contact for any questions relating to this memorandum or for any other matters relating to the protection of personally identifiable information is (b)(6) Director, Defense Privacy Office, (b)(6)

Michael B. Donley
DoD Senior Privacy Official