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

ADMINISTRATION AND
MANAGEMENT

FEB 07 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Appointment of a Senior Official for Privacy and Issuance of Revised Privacy Program Compliance Reporting Requirements

The Department of Defense (DoD) continues its commitment to protect the privacy of an individual's personally identifiable information. The Federal Government has increased its focus on the protection of the privacy of individually identifiable information and will likely continue to do so into the future.

This memorandum's purpose is two-fold. First, to ask DoD Military Department and Agency Leadership to appoint a Senior Component Official for Privacy, and to establish revised quarterly and annual reporting requirements. The DoD Component's appointee will work with me in the DA&M's role as the DoD Senior Agency Official for Privacy and with the Director of the Defense Privacy Office to build a stronger and more viable Privacy Program for the Department of Defense. The selected appointee should be in a Senior Executive Service (SES), General or Flag Officer grade position. Responsibilities are outlined in Attachment 1.

Second, the increased focus on the protection of personally identifiable information necessitates analysis of data to allow DoD to assess its overall compliance with the Privacy Act and other federal privacy requirements. The DoD 5400.11-R, DoD Privacy Program Directive established the Defense Privacy Program and the DoD Memorandum titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", dated September 21, 2007 augmented those requirements with new DoD policies designed to strengthen the program. Attachment 2 establishes new requirements for the quarterly and annual Federal Information Security Management Act (FISMA) reporting to the Defense Privacy Office to facilitate an ongoing assessment of compliance.

Attachment 3 lists the current organizational alignment of the service components Privacy Offices.

Questions regarding these policy requests should be directed to Samuel Jenkins, Director, Defense Privacy Office at (703) 607-2943 or via email at DPO.Correspondence@osd.mil.

Michael B. Donley
Director

Attachments:
As stated

Attachment 1 – Responsibilities of the Senior Component Officials for Privacy

Component responsibility and accountability for implementation of information privacy protections, including compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act and other federally mandated information privacy policies.

Take appropriate steps to protect personal information from unauthorized use, access, disclosure or sharing, and to protect or collaborate with appropriate offices in the protection of associated information systems from unauthorized access, modification, disruption or destruction.

Oversight of your component's compliance efforts including the review of components information privacy policies and procedures to ensure that they are comprehensive and up-to-date. Where additional or revised procedures may be called for, working with the relevant agency offices in the consideration, adoption, and implementation of such policies and procedures.

Ensure the component's employees and contractors receive appropriate training and education regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information.

Have a central policy making role in the component's development and evaluation of legislative, regulatory, and other policy proposals which implicate information privacy issues, including those relating to the component's collection, use, sharing, and disclosure of personal information.

Attachment 2 – Revised Privacy Program Reporting Requirements

With an increased focus on protection of Personally Identifiable Information (PII) the Defense Privacy Office has determined the need to initiate new reporting requirements to allow the department to assess its overall compliance with the Privacy Act and other federal privacy requirements. Currently, components report the number of breaches occurring in each quarter involving the loss, theft or compromise of personally identifiable data. This report is currently submitted to the Defense Privacy Office the first day of the last month of each quarter.

New quarterly reporting requirements include:

Privacy Act (PA) Systems of Records Notices Review. OMB Circular A-130, Management of Federal Information Resources, establishes managerial, procedural and analytical guidelines for maintaining information records for individuals. One requirement is that PA Systems of Records Notices be reviewed biennially to ensure that it accurately describes the system of records and the data collected is accurate, relevant, timely and complete. The review shall consist of 12 ½% of a components Systems of Records Notices and the status of completion of that review reported quarterly.

Routine Use and Exemption reviews. Systems of Records routine use disclosures and promulgated exemption rules require review every four years. The routine use disclosures associated with each system of records shall be reviewed to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information. The exemption rule review is to determine whether the exemption is still needed. Status of routine use and exemption reviews shall be reported when conducted as a part of the above system review.

Efforts to reduce use of Social Security Numbers (SSN). Each component shall indicate and report findings of the efforts they have attempted or successfully implemented to reduce the use of an individual's SSN in their systems or processes.

Reports of Inspections. Components are to report the results of inspections conducted by DoD and Component IG and other oversight bodies on their privacy program to include:

- Component Privacy Program inspected,
- Identified discrepancies, irregularities and significant problems, and
- Remedial actions taken to correct problems identified

New Annual Reporting Requirement:

Training Completion Certification. The DoD 5400.11-R requires privacy training for personnel assigned, employed, and detailed, including contractor personnel and individuals having primary responsibility for implementing the DoD Privacy Program. The DoD Memorandum titled Safeguarding Against and Responding to the Breach of Personally Identifiable Information, dated September 21, 2007 established the requirement that DoD components shall ensure their personnel receive Privacy Act training as a prerequisite before allowing access to DoD systems.

The training categories are:

Orientation Training. Training that provides individuals with a basic understanding of the requirements of the Privacy Act as it applies to the individual's job performance. The training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

Specialized Training. Training that provides information as to the application of specific provisions of this instruction to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, IT professionals, and any other personnel responsible for implementing or carrying out functions under this instruction.

Management Training. Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding the Privacy Act Program.

Privacy Act Systems of Records Training. Ensure all individuals who work with a Privacy Act system of records are trained on the provisions of the Privacy Act systems of records notice and this instruction. Stress individual responsibilities and advise individuals of their rights and responsibilities under this instruction.

Annual Refresher Training. Shall be provided to ensure employees and managers, as well as contractor personnel, continue to understand their responsibilities.

For each of the above training categories, report that the Component has provided appropriate training and documented certification from all persons required to take required training.

The Defense Privacy Office shall, when necessary, revise current and establish additional reporting requirements in support of the Privacy Program.

Attachment 3 – Present Organizational alignment of Service Component Privacy Offices

Review of the current organizational placement of the Service component's privacy official reveals that there is no consistency in this assignment. For example:

- Army: Records Management and Declassification Agency, Army Headquarters Services, Administrative Assistant

  Navy: Under reorganization to the CIO.

  Air Force: Information Assurance Branch, Policy and Resources Directorate, Chief Warfighting Integration and CIO

- Marine Corps: Security and Information Management Branch, Administration and Resource Management, Director, Marine Corps Staff