Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
CIO	Chief Information Officer
DITPR	DoD Information Technology Portfolio Repository
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
IA	Information Assurance
IT	Information Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 13, 2007

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DOD CHIEF INFORMATION OFFICER
DIRECTOR OF ADMINISTRATION AND MANAGEMENT

SUBJECT: Report on Audit of DoD Privacy Program and Privacy Impact Assessments (Report No. D-2007-099)

We are providing this report for review and comment. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer comments were fully responsive to twelve recommendations and partially responsive to three recommendations. We request additional comments from the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer on Recommendations C.1.a., C.2.a., and C.2.c. The Director of Administration and Management comments were fully responsive to one recommendation, partially responsive to two recommendations, and not responsive to seven recommendations. We request additional comments from the Director of Administration and Management on all recommendations with partial or not responsive comments. The Naval Postgraduate School comments were fully responsive and do not require additional comment. Therefore, we request that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and Director of Administration and Management provide comments by July 13, 2007.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AudROS@dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-8966) or Mr. Robert R. Johnson at (703) 604-9024 (DSN 664-9024). See Appendix D for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Wanda A. Scott
Assistant Inspector General
Readiness and Operations Support

Department of Defense Office of Inspector General

Report No. D-2007-099 **June 13, 2007**
(Project No. D2006-D000AL-0087.000)

DoD Privacy Program and Privacy Impact Assessments

Executive Summary

Who Should Read This Report and Why? The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer; Director of Administration and Management, Office of the Secretary of Defense; Director, DoD Privacy Office; and Privacy and Chief Information Officers of the Military Departments and DoD Components should read this report to obtain information about the implementation of the DoD Privacy and Privacy Impact Assessment Programs. This report discusses how DoD Components may be operating information systems that may not prevent the compromise and misuse of the public's personally identifiable information.

Background. In establishing the Privacy Act of 1974, Title 5 U.S.C. § 552a (as amended), Congress found that the right to privacy is a personal and fundamental right protected by the Constitution of the United States. The intent of the Privacy Act is to require Federal agencies to protect individuals against unwarranted invasions of their privacy through limiting the collection, maintenance, use, and disclosure of personal information about them. The Act requires that Federal agencies establish information practices that restrict disclosure of personally identifiable records and grants individuals increased access to agency records maintained on them.

The Office of Management and Budget required agency heads to designate a senior official within the agency to assume primary responsibility for privacy policy. The Director, Administration and Management, Office of the Secretary of Defense, is the designated DoD Senior Privacy Officer. The Director is required to report annually to the Office of Management and Budget on the DoD Privacy Program. The annual privacy report is currently included as an appendix to the DoD statutory report prepared for section 3545, Public Law 107-347, Title III, "Federal Information Security Management Act (FISMA)," December 17, 2002, of the E-Government Act of 2002.

The E-Government Act additionally requires that Federal agencies protect the collection of personal information in Federal government information systems by requiring that agencies conduct Privacy Impact Assessments. A Privacy Impact Assessment is an analysis of how personal information is collected, stored, shared, and managed in Federal information technology systems. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer is the principal staff assistant for information technology matters relating to DoD Privacy Impact Assessments.

We visited officials from the offices of the Defense Privacy Officer and the DoD Chief Information Officer, the Departments of the Army, the Navy, and the Air Force, the Defense Threat Reduction Agency, the Washington Headquarters Service, and the TRICARE Management Activity and 12 subordinate program offices responsible for the security and privacy of the specific information technology systems selected for review.

Results. We performed the audit to determine whether DoD Components reported consistent and valid information to the Office of the Secretary of Defense, the Office of

Management and Budget, and the Congress regarding management and protection of personal information related to the DoD Privacy Program. We also evaluated DoD compliance with Privacy Impact Assessment requirements and determined whether safeguards were established to prevent the compromise and misuse of personal information during its storage or transfer and were in accordance with Office of Management and Budget and DoD guidance implementing the Privacy and E-Government Acts.

DoD Components did not consistently implement Privacy Program policy for reporting, collecting, safeguarding, maintaining, using, and disseminating personal information. Specifically, DoD Components did not prepare system notices for systems of records, mark documents with mandatory privacy statements, designate privacy officer responsibilities, or conduct privacy training. As a result, the personal information contained in DoD information systems could be vulnerable to access by unauthorized personnel, and/or for unauthorized purposes (finding A).

DoD Components did not comply with the requirements of the E-Government Act of 2002 Privacy Impact Assessment program. Specifically, DoD Components did not establish responsibilities for conducting, reviewing, approving, and reporting Privacy Impact Assessments or posting those assessments to public Web sites. As a result, DoD information systems may not conform to DoD and Federal policies that protect handling, collecting, maintaining and disseminating privacy information. Additionally, DoD Components may be operating information systems that may not be designed to prevent the compromise and misuse of the public's personally identifiable information (finding B).

DoD Components did not complete Privacy Impact Assessments for information systems containing personally identifiable information or accurately report Privacy Impact Assessment information in the DoD Information Technology Portfolio Repository. As a result, Component Chief Information Officers could not report accurate information from the DoD Information Technology Portfolio Repository to the DoD Chief Information Officer, the Office of Management and Budget, and the Congress. Additionally, security risks associated with the protection of personal information may not be evaluated, leaving the systems and the public's information vulnerable to compromise or misuse (finding C).

See the Findings section of the report for the detailed recommendations.

We found weaknesses in the DoD Component's Management Control Programs for reporting Privacy Impact Assessment information in the DoD Information Technology Portfolio Repository and implementing privacy programs. For specific results of those weaknesses, see the Finding sections of the report. The recommendations, if implemented, will correct the identified weaknesses.

Management Comments and Audit Response. The Assistant Secretary of Defense for Networks and Information Integration, Deputy Chief Information Officer concurred with 14 recommendations and partially concurred with 1 recommendation. However, the Assistant Secretary of Defense for Networks and Information Integration, Deputy Chief Information Officer comments were fully responsive to 11 recommendations and only partially responsive to 4 recommendations. We agreed with the proposed actions for establishing internal controls, evaluating the inventory of systems, and implementing automated controls in the DoD Information Technology Portfolio Repository, but we request additional details on the actions. The DoD Senior Privacy Official, Office of the Director of Administration and Management generally concurred with the findings but

not with the recommendations. The comments stated that the Component Federal Information Security Management Act Privacy reporting, which includes assessing whether training programs are ensuring that personnel are generally familiar with privacy policies, is a more effective tool for overseeing and reviewing Component compliance with program requirements. The comments also stated that biannual certification requirements would not remedy the training problems identified in the report. The comments repeatedly stated that the current DoD Regulation on Privacy provides guidance on training, that the revised Regulation has been expanded to provide additional guidance as well, that Chief Information Officers do not have a direct role in the Privacy Program, and that Chief Information Officers do have a critical role to play regarding Privacy. Additionally, the comments stated that neither the Privacy Act nor the DoD guidance requires that a Privacy Act statement be provided by a third party who is furnishing information about an individual. We determined one of the DoD Senior Privacy Official's comments to be fully responsive, two comments as partially responsive, and seven comments as not responsive. Therefore, we request that the Director of Administration and Management provide additional comments on these recommendations by July 13, 2007.

The Chief of Staff, Naval Postgraduate School concurred with the recommendations; therefore, no further comments are required. We request that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Director of Administration provide comments on the final report by July 13, 2007.

Although not required to comment, the Department of the Navy and the Department of the Air Force sent unsolicited comments. The Chief Information Officer, Department of the Navy concurs with the need to update the Department of the Navy Privacy Instruction to reflect changes in the management of the Privacy Program, policies, and practices. The Director, Information Services and Integration (Office of Warfighting Integration and Chief Information Officer), Department of the Air Force, concurs with the audit findings and recommendations associated with the Privacy Act Program and Privacy Impact Assessments. See the Findings section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Background

Privacy Act of 1974. In establishing the Privacy Act of 1974, Title 5, U. S. C. § 552a (as amended), Congress found that the right to privacy is a personal and fundamental right protected by the Constitution of the United States (see Public Law 93-579, 88 Stat. 1896, section 2). The objective of the Privacy Act is to balance the Government's need to maintain information about individuals with the requirement that agencies protect individuals' rights against unwarranted invasions of their privacy through limitations on the collection, maintenance, use, and disclosure of personal individuals' information. The Act requires Federal agencies to establish information practices that restrict disclosure of personally identifiable records and grant individuals access to agency records maintained on them.

The Office of Management and Budget (OMB) Memorandum 99-05 Attachment A, "Privacy and Personal Information in Federal Records" May 14, 1998, required agency heads to designate a senior official within the agency to assume primary responsibility for privacy policy. The Director, Administration and Management, Office of the Secretary of Defense, is the designated DoD Senior Privacy Officer and is responsible for implementing the DoD Privacy Program. The Director is required to report annually to OMB on the DoD Privacy Program. The annual privacy report is currently included as an appendix to the DoD statutory report prepared for Public Law 107-347, Title III, Section 301, 44 U.S.C. § 3545 "Federal Information Security Management Act (FISMA)," December 17, 2002, of the E-Government Act of 2002.

E-Government Act of 2002. The E-Government Act requires that Federal agencies protect the collection of personal information in Federal Government information systems by requiring that agencies conduct Privacy Impact Assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in Federal information technology systems. OMB Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003, provides guidance to Federal agencies for implementing the privacy provision of the E-Government Act. OMB requires that Federal agencies conduct reviews of how information about an individual is handled within their agency when IT is used to collect, store, share, and manage personally identifiable information.

The Assistant Secretary of Defense Networks and Information Integration/DoD Chief Information Officer (CIO) is the principal staff assistant for information technology matters relating to DoD PIAs and is responsible for issuing guidance for conducting, reviewing, and publishing PIAs. Deputy DoD CIO Memorandum, "Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance," October 28, 2005, requires that system owners conduct a PIA on "all new or significantly altered Information Technology (IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public - excluding information on DoD personnel)." The DoD PIA Guidance requires that the Component CIO review and approve PIAs and forward approved PIAs to the DoD CIO and OMB.

We reviewed the Privacy and CIO offices for DoD, the Departments of the Army, the Navy, and the Air Force, the Defense Threat Reduction Agency, the TRICARE Management Activity, and the Washington Headquarters Service 12 subordinate program offices responsible for the security and privacy of the individual systems selected for review. We selected 18 systems for which PIA information was reported in the DoD Information Technology Portfolio Repository (DITPR). DITPR is, by policy, the Department's authoritative unclassified inventory of IT systems and the repository for system information used to meet a wide variety of internal and external reporting requirements.

Objectives

The overall objective of the audit was to determine whether DoD Components report consistent and valid information to the Office of the Secretary of Defense, OMB, and Congress regarding management and protection of personal information related to the DoD Privacy Program. We evaluated DoD compliance with PIA requirements and determined whether safeguards were in place that would prevent compromise and misuse of personal information while stored or while in transfer and whether they were in accordance with the OMB and DoD guidance. We also reviewed the Management Control Program as it related to the overall objective. See Appendix A for a discussion of audit scope and methodology and prior audit coverage related to the overall objective.

Review Of Internal Controls[1]

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We performed tests of the Management Control Program by performing the procedures used to accomplish our objectives. The objective was to determine whether DoD Components report consistent and valid information to the Office of the Secretary of Defense, OMB, and Congress regarding management and protection of personal information related to the DoD Privacy and PIA programs. By performing the procedures to review those programs, we, in effect, tested the Management Control Program for the DoD Privacy and PIA programs.

[1] Our review of the internal controls was done under the auspices of DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996. We continued using these directives because they were still in effect at the time of the audit announcement. DoD Directive 5010.38 was cancelled on April 3, 2006. DoD Instruction 5010.40 was reissued on January 4, 2006 as "Managers' Internal Control (MIC) Program Procedures."

Adequacy of Management Controls. We found weaknesses in the DoD Components' Management Control Programs for reporting PIA information in the DoD Information Technology Portfolio Repository and implementing privacy programs. For specific results of those weaknesses, see the Findings section of the report. The recommendations, if implemented, will correct the weaknesses. We will provide a copy of the final report to the senior official responsible for management controls at the DoD Components.

Adequacy of Management's Self-Evaluation. Our review revealed weaknesses with the Management Control Program for the Army, Navy, Air Force, Defense Threat Reduction Agency, and Washington Headquarters Service. With the exception of the Air Force, all Components reviewed conducted self-assessments of their Management Control Program. However, none conducted a review of either the privacy program or the PIA program. The Air Force had not conducted any self-assessments since FY 2004.

A. DoD Privacy Program

Operation of the current decentralized DoD Privacy Program is not effective because DoD Components did not ensure timely and uniform implementation of privacy program policy for reporting, collecting, safeguarding, maintaining, using, and disseminating personal information. Specifically, DoD Components did not consistently prepare system notices for systems of records, mark documents with mandatory Privacy Act statements, designate privacy officer responsibilities, or conduct privacy training. These conditions occurred because neither the DoD Privacy Office nor the DoD Components established oversight mechanisms and provided resources necessary for effective program execution. As a result, the personal information contained in DoD information systems could be vulnerable to access by unauthorized personnel, and/or for unauthorized purposes.

Privacy Act Program

DoD Components did not consistently implement privacy program policy for reporting, collecting, safeguarding, maintaining, using, accessing, amending, and disseminating personal information. Specifically, DoD Components did not prepare system notices for systems of records, mark documents with mandatory privacy statements, designate privacy officer responsibilities, or conduct privacy training in a timely and uniform manner.

System Notices. DoD Regulation 5400.11, "Privacy Program," August 1983, requires that DoD Components prepare system notices for systems of records containing personal information retrieved by name or personal identifier, such as an address, social security number, or telephone number. A system of records is a group of records under the control of a DoD Component from which information is retrieved by an individual's name or other personal identifier. DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004, and DoD Regulation 5400.11-R requires that DoD Components:

- submit system notices to the DoD Privacy Office for review and submission to the Federal Register[2] for publication;
- include a privacy statement on forms used to collect personal information and retained in a system of records by personal identifier; and

[2] Published by the Office of the Federal Register, National Archives and Records Administration, the Federal Register is the official daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents.

- establish formal training programs for individuals involved in the design, development, operation, and maintenance of any system of records.

Implementation of these requirements was inconsistent across DoD Components.

Army. Army Regulation 340-21, "The Army Privacy Program," July 5, 1985, requires that privacy officials ensure system notices are properly described in a published notice in the Federal Registry for new systems or systems undergoing major changes. The July 1985 regulation had not been updated to reflect the 2004 DoD Directive requirement that systems managers submit system notices through their Component's Privacy point of contact to the Defense Privacy Office for publication in the Federal Registry. Of the three Army locations visited, one location could not identify the system notices published in the Federal Registry for their systems of records. The remaining two Army locations provided a complete list of their systems of records and the corresponding system notices.

Navy. SECNAV Instruction 5211.5E, "Department of the Navy Privacy Program," December 28, 2005, requires that privacy officers and system managers prepare system notices, submit notices to the Department of the Navy Privacy Officer and DoD Privacy Office for review, and publish approved notices in the Federal Register before collecting or maintaining privacy-protected information. Of the three Navy locations visited, one was creating an inventory of systems of records to determine the number of system notices to prepare and publish for the identified systems. At two other Navy locations, the activity's privacy officer, in consultation with system owners, had prepared system notices for systems of records maintained.

Air Force. Air Force Instruction 33-332, "Privacy Act Program," January 29, 2004, requires that system managers prepare and submit system notices through their Major Command Privacy Officer to the Air Force CIO/Privacy Office. The Air Force CIO/Privacy Office then submits the system notice to the Defense Privacy Office for publication in the Federal Register for new and changed systems. The Instruction states that system notices are intended to inform the public of the types of records the Air Force maintains. The Instruction requires that the public have an opportunity to comment on the system notice before system managers implement or make changes to the system. Of the three Air Force locations visited, two locations could not identify system notices for the systems of records under review. The third location provided a complete list of their systems of records and the corresponding system notices, which had been published in the Federal Registry following review by the DoD Privacy Office.

Defense Agencies. The Washington Headquarters Service, the TRICARE Management Activity, and the Defense Threat Reduction Agency could identify their system of records and the corresponding system notices. Additionally, the three DoD agencies updated system notices in the Federal Registry as required.

Privacy Act Statements. DoD Regulation 5400.11-R, "Privacy Program," August 1983, requires that DoD Components include Privacy Act statements on

forms that collect personal information and maintain them in an associated system of records. DoD Regulation 5400.11-R also requires that DoD Components revise or add Privacy Act statements to forms that non-DoD agencies issue without Privacy Act statements before using the form to collect personal information. At the military activities visited, administrative personnel maintained numerous paper-based systems of records consisting of personnel forms with personal information. The forms, however, did not always contain a Privacy Act statement as required or it was not prominently displayed. Additionally for forms completed by supervisors or administrative personnel regarding other individuals, a required Privacy Act statement would enable these supervisors or administrative personnel to make informed decisions regarding the necessity of continued inclusion of selected personal information on these forms. For example, we found Department of the Army Form 1256, "Incentive Award Nomination and Approval," without any evidence of a Privacy Act statement being provided on the form or as an attachment, despite inclusion of names and other personal identifiers. The three DoD agencies reviewed, however, did implement policies or procedures to ensure the proper use of Privacy Act statements.

We also found that the military activities used non-Component-generated forms that did not include a Privacy Act statement before collecting the personally protected information. For example, the Army, Navy and Air Force used non-DoD Standard Form 50-B, "Notification of Personnel Action;" OMB Form No. 3206-0160, "Health Benefits Registration;" and Standard Form 2817, "Life Insurance Election Federal Employees Group Life Insurance Program." See Appendix B for a list of the forms containing personal information, which we found filed in a system of records, retrieved by personal identifier that did not contain a required privacy statement.

Privacy Officer Responsibilities. The Army, Navy, and Air Force privacy guidance requires that activity privacy officers administer privacy programs and implement Privacy Act requirements. We found that privacy officers at military activities did not or could not always address Privacy Act requirements. In addition, not all privacy officers had received formal management-level privacy training. For example, the Staff Judge Advocate at one Navy location was designated as the Privacy Act Officer in July 2003 as an additional duty, but did not begin complying with Privacy Act requirements for systems of records and system notices, privacy training, and Privacy Act Program assessments until April 2006.

At one Air Force Command, the Acting Privacy Officer appointed in April 2006 was also designated as the Freedom of Information Act (FOIA) officer and was expected to perform both duties while fulfilling other full-time work requirements. This Acting Privacy Officer could not verify whether system owners had prepared systems notices for the Command's systems of records we reviewed. At another Air Force Command, the Privacy Officer position was filled as an acting position for 2 years and the incumbent also fulfilled the responsibilities of another regular full-time position. The Acting Privacy Officer could not match the system notices to the IT systems of records we reviewed. In June 2006, following completion of on-site audit fieldwork, the Command hired a dedicated privacy officer.

At one Army location, the Privacy Officer who was appointed in October 2004 was responsible for the FOIA program in addition to other full-time duties. The Privacy Officer did not receive management-level Privacy Act training. At another Army location, the appointment of a Command Privacy Officer was pending, although we identified an official who was assigned privacy responsibilities for a division within the Command. At the third Army location, the Privacy Officer, appointed in July 2005, had not received any formal management-level privacy training.

The three DoD agencies reviewed designated privacy officers to administer their privacy programs. The Defense Threat Reduction Agency and TRICARE Management Activity's Privacy Officers oversee dedicated staff members who administer privacy requirements. The Washington Headquarters Service Privacy Officer is responsible for all privacy requirements.

Privacy Training. Of 12 locations visited, 10 had not implemented a job-specific privacy training program for employees and contractors directly involved with protecting personally identifiable information or IT systems containing such information. The Privacy Act requires that agencies maintaining systems of records establish rules of conduct for individuals involved in the design, development, operation, or maintenance of systems of records. DoD Regulation 5400.11-R establishes requirements for orientation, specialized, and management training for individuals involved with systems of records. Although the Regulation does not require all employees to be trained, such training would provide individuals with a basic understanding of DoD privacy requirements as they apply to the individual's job performance. The training would also provide managers of operational programs and activities with information on privacy implications.

Based on the information we received during interviews with privacy officials from the Military Departments and DoD agencies, we identified a lack of awareness of Privacy Act requirements. Additionally, the level of training varied by location. Of the 12 locations reviewed, privacy officials at 3 locations did not conduct training on privacy requirements and although privacy training was conducted at another 8 locations, the Privacy Officer did not document the requirements of the program or identify the types of training required for all levels of personnel including specialized and management training. The remaining location implemented and documented a privacy training program that included training for all levels of personnel.

Military Departments. The Departments of the Army and the Navy did not require privacy training for all personnel. Additionally, Army Regulation 340-21 is void of any requirements for privacy training. In December 2005, for the first time, the Air Force required Air Force personnel to complete privacy training using an on-line portal. The Air Force, however, in April 2006, rescinded the training requirement because the on-line portal could not accommodate the volume of users taking the training. Further, some Air Force personnel did not have access to a computer to take the training and, finally, the on-line curricula did not cover all elements that the Privacy Act requires.

DoD Agencies. While the three DoD agencies that we reviewed conducted and documented some form of privacy training, the frequency and sophistication of the training varied. The Defense Threat Reduction Agency implemented mandatory annual privacy awareness training in August 2003. Privacy awareness training is also conducted at the Washington Headquarters Service, and in August 2006, the Privacy Officer obtained approval to mandate annual computer-based privacy training. Implementation of the training is expected by August 2007. However, the Defense Threat Reduction Agency and Washington Headquarters Service did not implement specialized and management privacy training requirements for all employees requiring additional privacy training. At the TRICARE Management Activity, privacy training is required annually and specialized employees and managers also receive additional training.

OMB Memorandum M-06-15, "Safeguarding Personal Identifiable Information," May 22, 2006, re-emphasizes the responsibilities for Federal agencies under law and policy to safeguard personally identifiable information and train employees on their responsibilities regarding personal information. OMB Memorandum M-06-15 also requires that Federal agencies remind employees of specific responsibilities for safeguarding personally identifiable information within 30 days as well as the rules for acquiring and using protected information as well as the penalties for violating Privacy Act rules.

DoD Components should treat privacy training as a priority and develop and distribute appropriate privacy training material to all DoD personnel. The Components should identify all employees and contactors involved with protecting personally identifiable information, require that they complete annual privacy awareness training, and document completion of that training. Lastly, Components should require that personnel in sensitive, specialized, and management positions receive privacy training appropriate for their positions of trust. The Component should clearly specify the requirements for privacy training at each level and document the completion of all training for each individual trainee level.

Program Oversight and Resourcing

The Military Departments' privacy officers did not actively oversee the Departments' privacy programs consistent with DoD Directive 5400.11 requirements, and many privacy officers performed dual roles, with privacy responsibilities not given the higher priority.

The Army's Privacy Officer is responsible for ensuring that the Department of the Army fulfills all Privacy Act requirements in addition to administering the Army FOIA program and the Quality of Information Program. The Army privacy staff consisted of one privacy specialist and one office chief with management responsibilities for FOIA, privacy and the Quality of Information Program. The privacy specialist position is currently vacant, and there is no plan to fill the position.

Similarly, the Navy's Privacy Officer is responsible for developing and implementing policy and provisions of the Privacy Act, developing a Navy-wide privacy training program, and conducting privacy reviews. Additionally, the Privacy Officer is the training oversight manager who is responsible for managing notices for the Navy and joint Navy and Marine Corps Privacy Act systems, chairs the Navy's Privacy Act Oversight Working Group, and coordinates all Navy PIAs before submitting them to the Navy CIO with a staff of four employees.

The Air Force Privacy Officer is responsible for providing guidance and assistance to the Air Force Major Commands and field operating activities to verify that information requirements developed to collect or maintain personal data conform to privacy standards. In addition, the Privacy Officer with one other person is responsible for the Air Force FOIA and PIA programs as well as the Federal Register liaison.

The Defense Threat Reduction Agency, TRICARE Management Activity, and Washington Headquarters Service each designated a privacy act officer and issued privacy program guidance. The privacy officers, however, have additional duties, such as FOIA and PIA, and do not always have the resources necessary to fulfill their privacy duties.

Insufficient oversight compromises the safeguards for personal information contained in DoD information systems and exposes personal information to access by unauthorized personnel for unauthorized purposes. Requiring DoD Components and activities to complete bi-annual certifications that Privacy Act program requirements were implemented and are being followed by Components may assist privacy officers in identifying resources needed for compliance in managing more robust privacy programs.

Conclusion

Federal agencies have a special duty to protect personally identifiable information. The increased focus on privacy following information losses at numerous Federal agencies has resulted in OMB placing additional requirements on already thinly resourced DoD privacy program staff, and the current decentralized program cannot provide an effective response. DoD privacy officials do not consistently implement safeguards and policies for protecting personal privacy information as required by the Privacy Act, and Component privacy officers do not oversee privacy programs within their Components. The personal information contained in DoD systems could be vulnerable to access by unauthorized personnel and individuals identified in systems of records vulnerable to identify theft and fraudulent activities. Effective oversight and administration of the DoD Privacy Act program is contingent on the allocation of sufficient resources and establishment of internal control mechanisms to verify accomplishments of the program's intent.

Management Comments on the Finding and Audit Response

DoD Senior Privacy Official Comments on Defense Privacy Office Oversight. The report does not acknowledge that the Defense Privacy Office has a number of mechanisms in place, similar to those used by the Office of Management and Budget in its oversight role for Federal Privacy, which permits the Defense Privacy Office to oversee the Component Privacy Programs. The Defense Privacy Office has a dedicated technical channel with Component Privacy officials that provides the Defense Privacy Office with information on Components and permits Components to surface problems when encountered. The Defense Privacy Office oversees Components by reviewing and approving Privacy Act system of records notices, which shows how well Components are complying with Privacy Act requirements. The Defense Privacy Office prepares the Department's FISMA Privacy Report based, in part, on input provided by DoD Components. In effect, Components are tasked to assess their programs. The resulting input provides the Defense Privacy Office with an opportunity to assess the current health of the Component's Privacy Program. The DoD Inspector General and Component Inspectors General are a way to oversee Components, a means that until now has not been used frequently.

Audit Response. We reviewed management comments and determined that report revisions were not required. Current Defense Privacy Office and Component oversight mechanisms failed to ensure that DoD consistently implemented Privacy Program policy for reporting, collecting, using, safeguarding, and maintaining personal information. Component Privacy offices could not always document that system record notices had been prepared for required systems; did not always consult with subordinate offices when preparing Component FISMA responses forwarded to Defense Privacy Office; and did not always conduct proactive oversight of subordinate Privacy offices. Periodic reviews of the DoD Privacy Program by the DoD Inspector General and Component Inspectors General are not a substitute for sound management controls and oversight of the Privacy Program.

DoD Senior Privacy Official Comments on Privacy Act Statements. The report identifies a number of forms that did not include a Privacy Act statement. However, Standard Form 2817 and Standard Form 1199A do contain a Privacy Act statement. For Form 2817, the Privacy Act statement is described at the top of page 1. For Form 1199A, the Privacy Act statement is located on the back of the Form under the heading "Please Read This Carefully." Finally, Standard Form-50-B does not require a Privacy Act statement as information is not being collected directly from the individual.

Audit Response. We reviewed management comments and determined that report revisions were not required. Our review of Component system of records containing completed Standard Form 2817 found the statement at the top of the page; "See Privacy Act statement on the back of part 3." However, we found no back page on the forms we reviewed. Likewise, when reviewing completed 1199A forms we did not find a back page. Requiring Privacy Act statements on forms like Standard Form-50-B when information is provide by a trained third

party would enable these trained third parties to make informed decisions on whether to continue including selected personal information on these forms.

Department of the Navy Comments on the Finding. Although not required to comment, the Department of the Navy CIO provided the following comments on finding A. The Department of the Navy CIO concurs that SECNAV Instruction 5211.5E should be updated to reflect changes in managing the Privacy Program, policies, and practices. The Instruction is under review and will incorporate recommendations from this audit report, as appropriate. The Department of the Navy Privacy Act and FOIA offices acted to reduce the threat to personally identifiable information and increase privacy awareness by updating the Privacy web site, identifying systems of records on the web site, listing all changes to systems on the Privacy web site, developing and posting Privacy training materials on the Privacy web site, revising SECNAV Instruction 5211.5E, forming Privacy working groups to address best practices and policy, designating one full-time equivalent for IA to focus on PIAs and coordinate activities with the Privacy Act and FOIA offices, and reviewing one-third of the Department of the Navy's system inventory to ensure proper reporting. In addition, the Department of the Navy Deputy CIO (Marine Corps) is drafting policy for a PIA process, for personnel management on personally identifiable information, and for reporting of loss or compromise of personally identifiable information.

Audit Response. We reviewed the Department of the Navy comments and acknowledge the progress made to improve operations within the Navy Privacy Program.

Recommendations, Management Comments, and Audit Response

Revised Recommendations. We revised the recommendation to clarify our position that the responsibility for addressing Finding A recommendations resides with the Director of Administration and Management, Office of the Secretary of Defense.

We recommend that the Director of Administration and Management, Office of the Secretary of Defense:

a. Modify DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004, to require the Secretaries of the Military Departments and DoD Component heads to:

(1) Provide bi-annual certifications that the requirements for the Privacy Act training program, system of records, system notices, and Privacy Act statements have been implemented and are being followed, and forward the certificates to the Defense Privacy Office for review and retention.

Management Comments. The DoD Senior Privacy Official generally concurs with the findings but not with the recommendations. The Defense Senior Privacy Official stated that the Components are now under an affirmative obligation to ensure that the Program mandates are met. The Defense Senior Privacy Official also stated that biannual certification requirements would not remedy the problems identified in the report. The Component FISMA Privacy reporting is a more effective tool for overseeing and reviewing Component compliance with program requirements.

Audit Response. The DoD Senior Privacy Official's comments are not responsive. The FISMA Privacy reporting is primarily agency level inquiries. Component heads' FISMA reporting does not adequately reflect the condition of DoD Privacy operations because Component FISMA reports do not always include information from field Privacy offices. Privacy officers at all levels should report and certify information on the operation of their Privacy programs. The information should be submitted to the Component head who reviews and validates that information before certifying the Component submission to the Defense Senior Privacy Official. We request that the Defense Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

(2) Require that Privacy Act statements are included on any DoD and non-DoD form used to collect personally identifiable information regardless of who provides the information.

Management Comments. The DoD Senior Privacy Official generally concurs with the findings but not with the recommendations. The Defense Privacy Office stated that the report points out that DoD Regulation 5400.11 requires forms, whether DoD or not, to contain a Privacy Act statement if the information is being collected directly from the individual and filed in a system of records. Neither the Privacy Act nor the DoD guidance requires that a Privacy Act statement be provided by a third party who is furnishing information about an individual.

Audit Response. The DoD Senior Privacy Official's comments are not responsive. We agree that neither the Privacy Act nor the DoD guidance require a Privacy Act statement to be provided by a third party who is furnishing information about an individual. However, forms completed by supervisors, administrative personnel, or other third parties regarding other individuals personal information should require a Privacy Act Statement to properly and promptly alert those responsible individuals about the sensitivity of and the need to safeguard the personal data. Use of the Privacy Act Statement will enable those individuals to make informed decisions and inquiries regarding the necessity of continued inclusion of selected personal information on such forms. Because personally identifiable information is provided by an external source or third party does not negate the need to protect that data from unauthorized or improper access. We request that the DoD Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

(3) Require that Privacy officers receive management Privacy training within 90 days of appointment and include the Privacy training requirement in performance standards established for Privacy officials.

Management Comments. The DoD Senior Privacy Official generally concurs with the findings but not with the recommendations. The Defense Privacy Office stated that DoD Regulation 5400.11 will be changed to incorporate training requirements. However, the proposal of incorporating a Privacy training requirement into the performance standards of Privacy officials will be evaluated as part of the DoD Privacy Program review.

Audit Response. The DoD Senior Privacy Official's comments are partially responsive. We disagree that further evaluation is necessary before incorporating Privacy training requirements into the performance standards of Privacy officials. We identified a Defense Agency that has incorporated Privacy training requirements into every employee's annual performance standards. This requirement clearly proved to be an effective way to ensure completion of Privacy training and promote increased Privacy awareness among the agency staff. We request that the Defense Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

(4) Require that individuals involved with implementing privacy requirements and/or handling personal information receive appropriate specialized and management training as identified in DoD Regulation 5400.11-R, "Privacy Program," August 1983.

Management Comments. The DoD Senior Privacy Official generally concurs with the findings but not with the recommendations. The Defense Privacy Office stated that the current DoD Regulation on Privacy includes guidance on such training. The revised Regulation, which is undergoing a final review, has been expanded to provide additional guidance as well.

Audit Response. The DoD Senior Privacy Official's comments are partially responsive. The DoD Regulation 5400.11-R, "Privacy Program," August 1983, outlines the basis for non-mandatory specialized and management training. However, establishing mandatory specialized and management privacy training requirements for DoD Components is crucial to ensure that individuals involved with implementing Privacy requirements and/or handling personal information are fully aware of the importance and nature of their respective positions. We request that the Defense Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

(5) Require annual Privacy Act awareness training for all DoD employees that includes a certification of completion.

Management Comments. The DoD Senior Privacy Official generally concurs with the findings but not with the recommendations. The Defense Privacy Office stated that the new DoD Regulation on Privacy will state that Privacy awareness training will be offered and conducted. How often the training is conducted will be at the discretion of the Components.

Audit Response. The DoD Senior Privacy Official's comments are not responsive. We understand that it is the duty of the Component to train its individuals on Privacy awareness. However, during our review, we discovered a lack of knowledge of Privacy Act requirements throughout DoD Component Privacy offices. The Privacy training varied in sophistication and frequency and was nonexistent at some locations. For example, one DoD agency established an effective Privacy program designed to ensure that all employees understood their rights to Privacy protection and responsibilities. However, at another DoD Component office we found no Privacy training in place to ensure these same Privacy rights and responsibilities. Privacy training should be given the same level of attentiveness as DoD annual ethics and security training requirements. We request that the Defense Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

b. Assess the DoD privacy program for staffing levels and resources required to enable privacy officials to effectively fulfill their privacy duties and recommend resource reallocations to the Secretary of Defense, Secretaries of the Military Departments, and DoD Component Heads as necessary to ensure a viable privacy program.

Management Comments. The DoD Senior Privacy Official generally concurs with the Findings but not with the recommendations. The DoD Senior Privacy Official agrees that Component staffing levels and resources should be assessed with a view of determining what can be done to enhance Program effectiveness. The DoD Senior Privacy Official stated that the assessment will be conducted as part of the DoD Privacy Program review.

Audit Response. Management comments are responsive. The DoD Senior Privacy Official agrees on the necessity to assess the DoD Privacy program for staffing levels and resources required and provided a review target completion date of the fourth quarter, FY 2007. No further comments are required.

c. Modify DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004, to require that Component Privacy officers, in coordination with the Component Chief Information Officers, support preparation of the certifications required in Recommendation a.

Management Comments. The DoD Senior Privacy Official generally concurs with the Findings but not with the recommendations. The DoD Senior Privacy Official stated that CIOs do not have a direct role in the Privacy Program, although they do have a critical role to play regarding Privacy. In effect, the Component Privacy Official relies on the Component CIO to develop the appropriate technical safeguards that will protect personally identifiable information in IT systems, thereby permitting the Component to comply with the Privacy Act, and implementing DoD and the Component authority.

Audit Response. Management comments are not responsive. The coordination between the Component Privacy officials and the CIOs is essential for the success of the Privacy Program. Establishing procedures to coordinate preparing, reviewing, and approving system record notices and establishing technical safeguards will advance awareness and compliance with Privacy requirements

throughout the DoD. We request that the DoD Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

(1) Develop an authoritative inventory of Component systems of records containing personally identifiable information.

Management Comments. The DoD Senior Privacy Official generally concurs with the Findings but not with the recommendations. The DoD Senior Privacy Official stated that the DoD Regulation 5400.11 requires the Defense Privacy Office to maintain an authoritative inventory of systems of records notices. The DoD Senior Privacy Official stated that the inventory is posted in the Defense Privacy Office website.

Audit Response. Management comments are not responsive. System owners could not always identify or substantiate that systems of records notices had been prepared for information technology systems and paper-based systems. Additionally, while systems owners were aware of systems of records that covered multiple systems, they could not always identify single systems covered by a blanket system of records notice. Component Privacy officers, in coordination with the Component CIOs, should develop and maintain systems of records inventory for all Component-owned systems. We request that the DoD Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

(**2) Prepare system notices for the inventory of systems of records maintained.**

Management Comments. The DoD Senior Privacy Official generally concurs with the Findings but not with the recommendations. The DoD Senior Privacy Official stated that CIOs do not have a direct role in the Privacy Program, although CIOs have a critical role to play regarding Privacy. The DoD Senior Privacy Official stated that the DoD 5400.11 requires system managers to prepare a system notice for any new, amended, or altered system and to forward that notice to the Component Privacy Official for review.

Audit Response. Management comments are not responsive. The recommendation discusses the need for the Component Privacy officers and CIOs to coordinate a review of system notices that the system owner prepared. DoD Component Privacy Officers could not always identify whether or not systems were covered by a system of records notice. Privacy officer and CIO coordination will benefit the system notice process by fostering increased communication and awareness. We request that the DoD Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

(3) Oversee subordinate privacy programs by conducting privacy reviews and verifying that privacy training is conducted at all required levels.

Management Comments. The DoD Senior Privacy Official generally concurs with the Findings but not with the recommendations. The DoD Senior Privacy Official stated that Component Privacy Officials are currently required to provide input for the FISMA Privacy Report, to review their Privacy Programs, to include assessing whether their training programs are ensuring that personnel are generally familiar with information Privacy laws, regulations, and policies and whether appropriate job-related training is being offered.

Audit Response. Management comments are not responsive. Component Privacy offices did not perform proactive oversight of subordinate Privacy programs; instead, efforts were focused on responding to subordinate office inquiries. The current DoD Directive 5400.11 does not direct Component Privacy offices to oversee subordinate Privacy programs. FISMA Privacy reporting is not an effective oversight tool for reasons stated in Recommendation a.(1), Audit Response. We request that the DoD Senior Privacy Official reconsider his position on the recommendation and provide additional comments on the final report.

B. Privacy Impact Assessments

DoD did not fully comply with the PIA requirements of the E-Government Act of 2002, and a significant portion of the DoD CIO community did not establish responsibilities for conducting, reviewing, approving, and reporting PIAs or posting PIAs to public Web sites. DoD did not comply with requirements of the Act because the ASD[NII]/DoD CIO and the Component CIOs did not provide timely guidance for implementing a DoD PIA program following enactment of legislation in December 2002. Also, the DoD CIO community did not follow safeguards or establish effective management oversight mechanisms to protect personally identifiable information. As a result, DoD information systems may not conform to DoD and Federal policies regarding privacy information and their operation may not be designed to prevent the compromise and misuse of the public's personally identifiable information.

E-Government Act of 2002

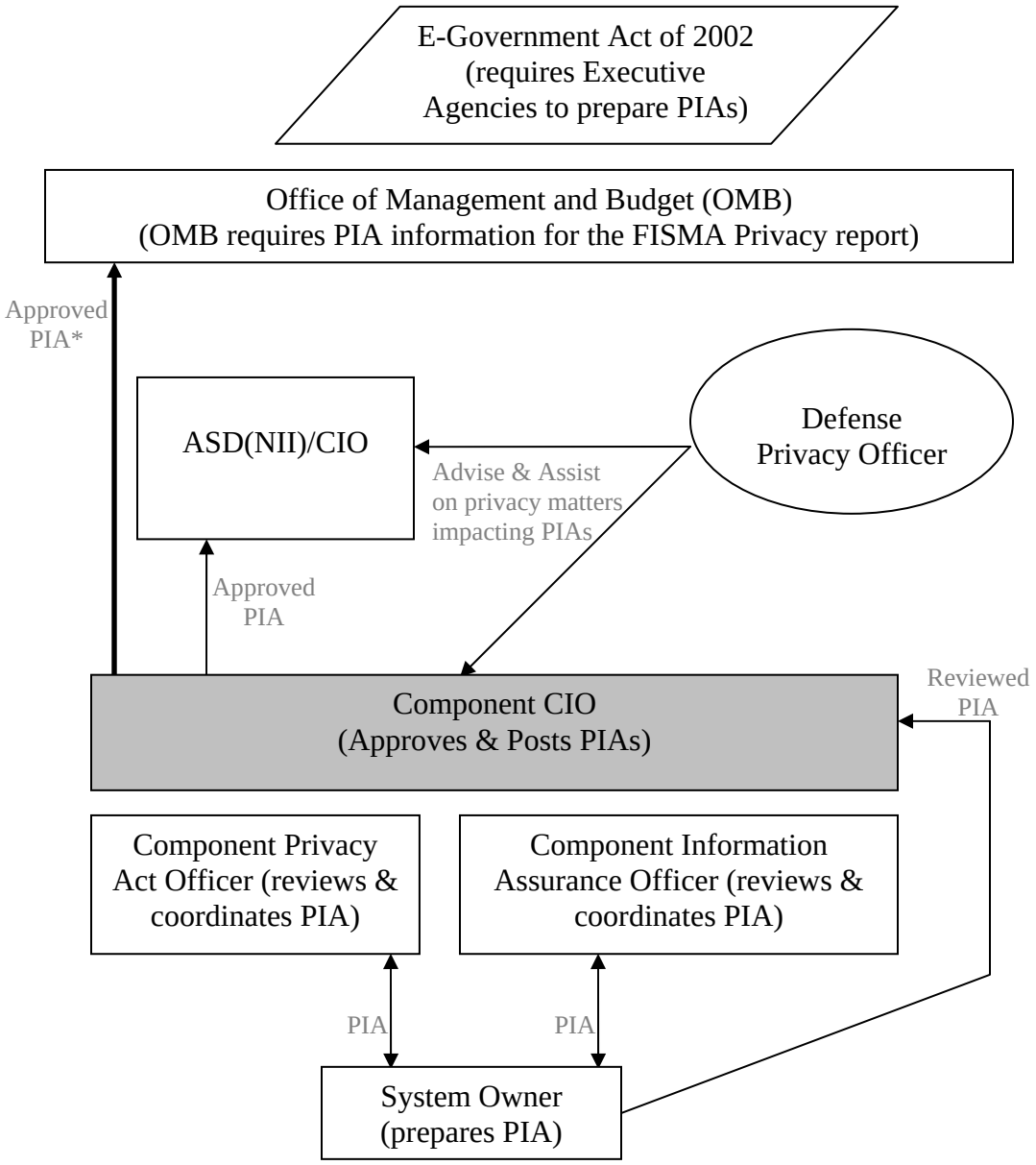
The E-Government Act establishes protections for the privacy of personally identifiable information as agencies implement an electronic Government that focuses on citizens. Personally identifiable information is information that directly identifies an individual, such as by name, address, social security number, telephone number, gender, birth date, or e-mail address. To accomplish this, the Act requires that Federal agencies conduct PIAs. A PIA addresses privacy factors for new or significantly altered IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public. Once complete, the Act requires that Federal agencies submit PIAs to OMB.

The E-Government Act also requires that OMB issue guidance to Federal agencies specifying the required content of a PIA. In September 2003, OMB issued OMB Memorandum 03-22 that implemented the privacy provisions of the E-Government Act. The DoD Deputy CIO issued PIA guidance implementing OMB Memorandum 03-22 for DoD Components 2 years later on October 28, 2005.

DoD did not fully comply with the PIA requirements of the E-Government Act. Although the DoD PIA Guidance included additional responsibilities for the review and coordination of a PIA at the Component level, the guidance partially contradicted the requirements of the E-Government Act. Specifically, the DoD PIA guidance requires that Component CIOs ensure that PIAs are properly developed and reviewed, approved and publicly accessible, and forwarded to OMB for IT systems and projects. The Act, however, requires that the Executive Agency CIO (the ASD(NII) for DoD) review PIAs before they are made publicly accessible. The DoD CIO delegation to the Component CIOs is inconsistent with the intent of the Act in that it does not provide for a Departmental-level PIA program. Further, the DoD CIO guidance does not specify the responsibilities of the DoD CIO for reporting PIA information to the DoD Senior Privacy Official for inclusion in the annual reporting to OMB. The diagram below depicts the

DoD decentralized process for conducting, reviewing, coordinating, and approving a PIA. A discussion of the process follows.

DoD PIA Process



* The E-Government Act requires that ASD(NII)/DoD CIO review PIAs and make them publicly available if practicable, and provide the Director of OMB a copy of the PIA for each system for which funding is requested. The DoD CIO, however, delegated that authority and responsibility to Component CIOs.

Privacy Impact Assessment Requirements

Components' CIOs did not establish responsibilities for conducting, reviewing, approving, and reporting PIAs or posting PIAs to public Web sites. The DoD PIA Guidance and OMB Memorandum 03-22 require that agencies conduct reviews about the handling of an individuals' information within an agency when agencies use IT for collecting new information, or when agencies develop or buy new IT systems that will handle collections of personally identifiable information. The DoD PIA Guidance and OMB Memorandum 03-22 also require that agencies describe how they handle information individuals provide electronically to the Government, so the public has assurance that the Government is protecting personal information.

PIA Responsibilities. DoD PIA Guidance assigns responsibilities and establishes a process for Component CIOs, privacy officers, and Information Assurance (IA) officials to use when completing, reviewing, approving, and posting PIAs. The Component privacy officer is responsible for reviewing and coordinating PIAs to identify and evaluate privacy implications. The IA official reviews and coordinates PIAs to assess compliance with DoD IA policies. As the PIA reviewing official, the Component CIO verifies that system owners complete PIAs and approves and submits the assessment to the DoD CIO and OMB, and posts the PIA on the Component's public Web site.

Army. In January 2006, the Department of the Army CIO (Army CIO) designated a department-level PIA official. The Army PIA official is responsible for adhering to the requirements of the DoD PIA program. Army Regulation 340-21, "The Army Privacy Program," however, has not been updated in more than 20 years, nor has supplemental Army guidance been provided for preparing and reviewing PIAs. A PIA program did not exist at two of the three Army locations visited. One system owner stated that he was not aware of the DoD PIA Guidance. At another location, the Privacy Officer, in addition to reviewing a PIA for privacy implications, also approved the PIA. None of the locations assigned responsibility to an IA official to review PIAs for compliance with IA policies.

In the absence of DoD guidance, the Army Corps of Engineers prepared a PIA using the General Services Administration PIA template as a guide. System owners completed the PIA before the DoD CIO issued the DoD PIA template in October 2005. The approved Corps PIA was sent directly to OMB, but not to either the Army or DoD CIO. Future Corps PIA development and submissions should be consistent with OMB and DoD guidance.

Navy. The Department of the Navy CIO (Navy CIO) designated an official responsible for the Navy's PIA program and stipulated that the Navy official must meet the requirements of the DoD PIA program. However, SECNAV Instruction 5211.5E did not include some of the PIA responsibilities in the DoD PIA Guidance. Although SECNAV Instruction 5211.5E requires that the Navy CIO provide guidance to Navy officials on PIAs and oversee policy and procedures that will ensure system owners conduct PIAs, the Instruction does not require that an IA official review PIAs for compliance with IA policies. The

Navy PIA official did not review, approve, or submit Navy PIAs to the DoD CIO or OMB because the Navy Components did not provide any PIAs for review.

We reviewed the implementation of the PIA program at three Navy locations and found that none assigned PIA responsibilities as the DoD PIA Guidance requires. System owners at one location stated that they did not assign PIA responsibilities because they were not aware that requirements existed. System owners at another location stated that they did not prepare any PIAs or assign responsibilities for PIA requirements because they determined that their systems do not require PIAs.

System owners at the third Navy location stated that they used the Navy's PIA template to prepare PIAs. System owners reviewed and submitted the PIA to the Navy Privacy Officer on December 15, 2005, for review. However, the DoD and Navy CIOs did not receive the PIA. The system owner did not track the status of the PIA after submitting the assessment to the Navy Privacy Officer. In addition to not tracking the status, the system owners did not require that the IA official review the PIA before submitting the assessment to the Navy Privacy Officer to determine compliance with IA policies. Further, SECNAV Instruction 5211.5E requires that the Navy CIO review and approve PIAs for the Navy, not the Navy Privacy Officer.

Air Force. Air Force Instruction 33-332 requires that system owners conduct PIAs. The Instruction requires that the Privacy Act office review the PIA and provide the assessment for final approval to both the major command and headquarters functional CIO. Once reviewed at the subordinate level, the Instruction requires the submission of the PIA to the Department of the Air Force CIO. In the Air Force, the Privacy Act officer and PIA officer are one and the same, and that official stated that Air Force Components did not submit PIAs to the Air Force CIO, the DoD CIO, or OMB because Air Force Components were not preparing PIAs. According to the Air Force Privacy/PIA Officer, system owners did not have any approved PIAs to submit for review as of August 2006.

We reviewed the PIA programs at three Air Force sites. None of those three commands assigned PIA responsibilities that the DoD PIA Guidance requires. System owners at two commands did not assign responsibilities or prepare a PIA because they were not aware of the requirements. As a result, the commands did not designate a PIA official or conduct systems evaluations that could determine whether their information systems require PIAs. A system owner at the third command is preparing the command's first PIA, which includes the system owner completing the PIA, the Records Management/Privacy Officer reviewing the PIA, and the functional CIO approving the PIA. The PIA process and Air Force Instruction 33-332 do not require that the IA official review the PIA for compliance with DoD IA policies. Air Force officials stated that they are planning to update Air Force Instruction 33-332 by December 2006. The updated Instruction will include the requirements of the DoD PIA program. The Air Force Privacy/PIA Officer also stated that since the audit teams initial visit, the Air Force has begun assigning PIA responsibilities Air Force-wide.

DoD Agencies. We reviewed the PIA programs at three DoD agencies. Of the three agencies, the Defense Threat Reduction Agency did not assign PIA

responsibilities in accordance with DoD PIA Guidance. That agency did not establish any PIA roles and responsibilities for individuals who must be involved in the PIA process. In the two remaining agencies, the TRICARE Management Activity and the Washington Headquarters Service processes were in place to determine whether their information systems require a PIA. Although that process was in place, the Washington Headquarter Service did not complete any PIAs or formally document the use of their process. The IA official, the Privacy Office, and CIO at both the Washington Headquarters Service and the TRICARE Management Activity were in place to review and coordinate PIAs during the approval process, which met the requirements of the guidance.

Component CIOs must ensure adherence to DoD PIA Guidance and assign PIA responsibilities within their agencies. Component CIOs should require that system owners submit system evaluations for the proper review. The Component CIOs should review system owner evaluations that include any determination that an assessment was not required. Component CIOs should ensure that PIA policy complies with the DoD PIA Guidance.

Posting PIAs to Public Web Sites. The guidance requires that each DoD Component maintain a repository of PIAs and post PIAs to a central location on the Component's public Web site. The PIA should remain posted until the Component terminates the system or no longer maintains information in identifiable form in the system. The DoD PIA Guidance also directs that the ASD(NII) maintain a DoD Web site that enables public access to approved PIAs or summary PIAs.

Although the ASD (NII)/DoD CIO Web site contains a PIA link, the link only provides access to a PIA request box (and no list of PIAs). The CIOs for the Army, Navy, and Air Force did not post approved PIAs to their Web sites because the CIOs did not receive any completed PIAs. In addition, both the Defense Threat Reduction Agency and the Washington Headquarters Service did not post PIAs to their Web sites because those agencies did not complete one. The TRICARE Management Agency posted a list of completed PIAs on its Web site. The Web site contained a link for viewers to request a copy of the PIAs. Only two Components, the Air Force and the TRICARE Management Activity, included the E-Government Act requirement to post PIAs to the agency's Web site in their guidance.

A DoD Component CIO must make PIAs available to the public and provide necessary guidance for doing so to their Component. The ASD(NII)/DoD CIO should have either posted any approved PIAs to their Web site or provided links to Component web sites for accessing them. Additionally, the ASD(NII)/DoD CIO should clarify the circumstances in which PIAs are to be made available to the public.

Management Oversight

DoD Components did not fully comply with requirements of the E-Government Act because ASD(NII)/DoD CIO and the Component CIOs did not provide timely

implementing guidance for a DoD PIA program following enactment of legislation in December 2002. Also, they did not implement safeguards or establish effective management oversight mechanisms to protect personally identifiable information by:

- thoroughly disseminating requirements for PIAs to DoD system owners;
- updating guidance to assign necessary responsibilities to officials reviewing, coordinating, approving, reporting, and posting PIA information;
- requiring that PIA officials complete training required for evaluating, completing, or submitting a PIA; and
- establishing effective internal control mechanisms to ensure compliance with PIA requirements.

CIO Oversight. The DoD PIA Guidance requires that the ASD(NII)/ DoD CIO serve as the DoD principal point of contact for any IT matters relating to PIAs. The guidance requires that the CIO provide Department-wide guidance on how to conduct, review, and publish a PIA. Military Departments and heads of DoD Components must establish policies and procedures that implement the guidance. DoD Components must also educate personnel on their responsibilities for protecting personally identifiable information. The CIO did not, however, issue the guidance until October 2005; two and one half years after the E-Government Act went into effect in April 2003. In addition, the DoD CIO and Component CIOs did not adequately oversee system owners who are required to conduct PIAs. As a result, systems owners at the Army, Navy, and Air Force stated that they were not aware of the DoD PIA Guidance.

Active oversight of the PIA process is important to guarantee that Component CIOs are implementing PIA programs and that system owners are conducting PIAs on required systems. Component CIOs should be overseeing the PIA program to determine that system owners secure, protect, and preserve the confidentiality of the information in identifiable form.

DoD PIA Guidance. The DoD PIA Guidance requires that DoD Components complete a PIA when developing or procuring an IT system or project that collects, maintains, or disseminates information in identifiable form on members of the public. The Guidance, however, does not require that DoD Components conduct a PIA on DoD information systems that collect and maintain personally identifiable information on DoD personnel. Although the PIA requirements of the E-Government Act permit exclusion of DoD personnel, privacy implications should be considered for any information system that collects personally identifiable information. OMB Memorandum 06-20, "FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," July 17, 2006, states that OMB encourages agencies to scrutinize their internal business processes for handling identifiable information about employees to the same extent they scrutinize processes and information handling procedures involving information collected from or about members of

the public, despite section 208 of the E-Government Act and OMB Memorandum 03-22 stating otherwise. By conducting PIAs on IT systems that collect information on DoD personnel, in addition to the public, individuals within DoD can be assured that their personally identifiable information is as secure as that of the general public.

Component CIOs did not disseminate DoD PIA Guidance throughout all levels of their Components. Of the 12 locations visited, 5 were not familiar with or had never received the DoD PIA Guidance before the audit. Of the five, four locations did not complete any PIAs and assign PIA responsibilities. The fifth location completed PIAs but the process used for reviewing, coordinating, and approving a PIA did not meet DoD requirements.

DoD Component PIA Guidance. DoD PIA Guidance requires that the Military Departments and heads of DoD Components establish policies and procedures that implement the DoD PIA Guidance and are consistent with OMB Memorandum 03-22.

However, Army Regulation 340-21 did not include any PIA requirements because the Regulation was more than 20 years old. An Army official stated that an update to the Regulation is in draft. During our review, the Army CIO was developing draft PIA guidance. SECNAV Instruction 5211.5E included some PIA requirements, but the Instruction did not include a requirement that an IA official review and coordinate PIA for compliance with DoD IA policy. The Instruction also did not require that the Component CIO post approved PIAs to their public Web site. On June 16, 2006, however, the Navy did issue PIA guidance, which requires Navy activities to perform PIAs on any new or significantly altered IT systems that collects information in identifiable form on Navy military and civilian personnel and members of the public. Although approved on January 29, 2004, Air Force Instruction 33-332 did not meet the requirements of the DoD PIA Guidance because it did not require that the IA official review the PIA for IA implications or designate the Air Force Privacy Official as the PIA reviewing official at the Air Force CIO. The Instruction also did not require that system owners send completed PIAs to the DoD CIO and OMB. One Air Force official stated that the Instruction will be updated by December 2006.

The Washington Headquarters Service and the Defense Threat Reduction Agency did not develop any PIA guidance, but the TRICARE Management Activity did. The TRICARE Management Activity developed the "TRICARE Management Activity Privacy Impact Assessments (PIAs)," February 10, 2006. The TRICARE guidance outlines responsibilities of officials, responsibilities for the PIA process, and instructions on how to manage completed PIAs.

PIA Training. Although DoD does not require PIA training, the DoD Deputy CIO memorandum of October 28, 2005, requires the Secretaries of the Military Departments and the heads of other DoD Components to "educate employees and contractors on their responsibilities for protecting information in identifiable form that is being collected, maintained, and disseminated by IT systems." Specific PIA training should be required at all levels. PIA training would enable individuals to understand when a PIA is required, the correct reporting structure

for processing a PIA, and systems requiring a PIA are properly reviewed to verify safeguards are in place that limit the risk that personal information will be compromised or lost. Of the 12 locations reviewed, the TRICARE Management Activity was the only DoD Component that had a formal PIA training program and the TRICARE Management Activity system owners were the most knowledgeable about the requirements for evaluating IT systems in relation to PIAs.

The implementation of PIA guidance and training is essential to protect personal information in information technology systems. The failure to implement PIA requirements could result in unauthorized disclosure of personal information causing significant harm to members of the public.

Conclusion

DoD information systems may not conform to DoD and Federal policies regarding privacy information, and DoD Components may be operating information systems that do not provide safeguards to prevent the compromise and misuse of the public's personally identifiable information. The Components should identify the CIOs as the officials responsible for PIAs. The CIO must disseminate the DoD PIA Guidance throughout the Components to ensure that Components complete PIAs, establish a process for reviewing and approving PIAs before forwarding the PIA to the ASD(NII)/DoD CIO and OMB; and post the PIA on the public Web site. ASD(NII)/DoD CIO, the Military Departments, and DoD Components need to develop additional, clarifying PIA guidance and oversee the implementation of the new and current guidance to ensure that the Component CIOs are implementing an effective PIA program. PIA training must be developed and provided to any individual involved in the PIA process to ensure that the requirements of the program are being met.

Recommendations, Management Comments, and Audit Response

B.1. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, in coordination with the Director of Administration and Management, Office of the Secretary of Defense/DoD Senior Privacy Official:

a. Determine the most appropriate management structure for overseeing a Department-level privacy and Privacy Impact Assessment program in accordance with the requirements of the E-Government Act of 2002 and Office of Management and Budget Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003, and subsequent Office of Management and Budget guidance for Privacy Impact Assessments and protection of personally identifiable information.

Management Comments. The ASD(NII)/DoD CIO concurred with this recommendation. Management reviewed the current management structure and determined that a decision to keep the current management structure appears to be most appropriate. The ASD(NII)/DoD CIO and the Office of the Director of Administration and Management work closely on protecting personally identifiable information and PIAs.

Audit Response. ASD(NII)/DoD CIO comments were partially responsive to the recommendation. We acknowledge the corrective actions taken by management to address deficiencies identified during this audit. Effective management of Privacy and PIAs is dependent on consistent coordination between the two offices. We request that both the ASD(NII)/DoD CIO and the Director of Administration and Management validate and approve the state of the current management structure for overseeing Privacy and PIAs in DoD.

b. Revise the charters of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Director of Administration and Management, Office of the Secretary of Defense/DoD Senior Privacy Official to reflect the conclusions reached under recommendation B.1.a.

Management Comments. The ASD(NII)/DoD CIO did not respond to the recommendation stating that this recommendation did not apply based on their comments on Recommendation B.1.a. The ASD(NII)/DoD CIO stated that current missions as recorded in DoD policies and regulations are appropriate.

Audit Response. The ASD(NII)/DoD CIO did not comment on this recommendation because they concluded a revision was not required to the current management structure. Based on our response to management comments to Recommendation B.1.a., we request that the ASD (NII) DoD CIO provide additional comments on the final report.

c. Revise Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance," October 28, 2005, to reflect actions taken in accordance with Recommendations B.1.a. and B.1.b. and to:

(1) Require that implementing guidance for the DoD Components' revised memorandum be reviewed and approved by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and issued within 60 days of publication of the revised Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer memorandum;

Management Comments. ASD(NII)/DoD CIO concurred with this recommendation. However, management recommends 120 days to issue the implementing guidance as opposed to 60 days.

Audit Response. ASD(NII)/DoD CIO comments were responsive to the recommendation. We concur with management's comments and the request for 120 days to issue the implementing guidance. No further comments are required.

(2) Require that all DoD Components forward PIAs to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer for review and approval;

Management Comments. The ASD(NII)/DoD CIO partially concurred with the recommendation, stating that Components will be required to submit their PIAs after they are approved at the Component level. DoD PIA guidance is expected to be updated by fourth quarter FY07 and will include this recommendation.

Audit Response. Although management partially concurred with the recommendation, their comments are responsive to the recommendation. We discussed this recommendation with ASD(NII)/DoD CIO, and we agree that management should review PIAs for completion after PIAs have been reviewed and approved at the Component level. No additional comments are required.

(3) Require that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, rather than Component Chief Information Officers be responsible for submitting approved Privacy Impact Assessments to the Office of Management and Budget;

Management Comments. The ASD(NII)/DoD CIO concurred with the recommendation. The revised DoD PIA guidance will incorporate this requirement.

Audit Response. The ASD(NII)/DoD CIO comments are responsive to the recommendation; therefore, no further comments are required.

(4) Require that all personally identifiable data for DoD employees be afforded the same level of assessment and protection provided to data for the general public;

Management Comments. Management concurred with the recommendation. ASD(NII)/DoD CIO will incorporate the recommendation into the revised PIA guidance.

Audit Response. The ASD(NII)/DoD CIO comments are responsive to the recommendation. We concur with management's comments with the understanding that revised PIA guidance will require PIAs for all systems that contain personally identifiable information on DoD employees and members of the public. No further comments are required.

(5) Clarify how the Privacy Impact Assessment request link on the Web site of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer is responsive to the requirement of the E-Government Act to make Privacy Impact Assessments publicly available; and

Management Comments. The ASD(NII)/DoD CIO concurred with the recommendation. The ASD(NII)/DoD CIO PIA website will display a link to each Component's PIA website that lists all PIAs after the DoD PIA guidance is revised in the fourth quarter of FY 07.

Audit Response. The ASD(NII)/DoD CIO comments were responsive to the recommendation; therefore, no further comments are required.

(6) Specify the target audience and nature of training that DoD Components are required to provide for Privacy Impact Assessments.

Management Comments. Management concurred with the recommendation. ASD(NII)/DoD CIO annually briefs the DoD resource managers on the PIA requirements for the major IT systems reported in the Exhibit 300s. By July 31, 2007, management will have reviewed the curriculums at the Defense Acquisition University and Information Resources Management College to determine whether PIA information is captured in their courses. Also by July 31, 2007, PIA training content will be added to the Defense Information Systems Agency Information Assurance training program and distributed DoD-wide.

Audit Response. ASD(NII)/DoD CIO comments were responsive to the recommendation; therefore, no further comments are required.

B.2. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer require that DoD Component CIOs:

a. Disseminate Office of Management and Budget Memorandum 03-22 and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer October 28, 2005, Privacy Impact Assessment guidance to all Component information technology system owners to assist them in conducting required Privacy Impact Assessments, pending receipt of revised DoD and DoD Component guidance;

Management Comments. The ASD(NII)/DoD CIO concurred with the recommendation. The estimated completion date for this task is May 31, 2007.

Audit Response. The ASD(NII)/DoD CIO comments were responsive to the recommendation; therefore, no further comments are required.

b. Advise subordinate Component Chief Information Officers and privacy officers that personally identifiable data for DoD employees should be afforded the same level of assessment and protection offered to similar data from the general public.

Management Comments. Management concurred with the recommendation. The revised DoD PIA guidance will incorporate this recommendation.

Audit Response. The ASD(NII)/DoD CIO comments are responsive. We concur that this action will be completed after the DoD PIA guidance is revised in the fourth quarter of FY 07. No further comments are required.

C. Reporting in the DoD Information Technology Portfolio Repository

DoD Components did not accurately report system status information in DITPR. This condition occurred because the ASD(NII)/DoD CIO and the Components did not have effective internal controls in place to validate the accuracy of the system status information posted in the various DITPR data elements. As a result, the DoD, OMB, and the Congress are making management and budgetary decisions based on unreliable reports generated from DITPR, the sole DoD-wide data repository for system information on the status of DoD information systems.

DoD Information Technology Portfolio Repository Guidance

The DoD CIO Memorandum, "Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SIPRNet IT Registry Annual Guidance for 2006," May 17, 2006 (DITPR Guidance), states that DITPR is the DoD's authoritative unclassified inventory of IT systems. DITPR is the repository for system information used to meet a wide variety of internal and external reporting requirements. For example, regularly scheduled reports driven by legislative or regulatory mandates using data from throughout DoD, annual reports required by other Federal departments, and ad hoc reports using a subset of data available in DITPR. DITPR is the DoD data source for, among other things, required reporting on system certification, FISMA, E-Authentication, PIA, and the Privacy Act, as well as the inventory of systems required by the Clinger Cohen Act and for Portfolio Management. DITPR requires that system owners answer "trigger" questions that determine whether certain data elements apply to their system. When a system owner answers yes to a trigger question, DITPR requires additional information. For instance, to determine whether system owners should enter PIA and Privacy Act information into DITPR, the system owner would answer yes to the question, "Does this system contain personally identifiable information?" If the questions do not apply, DITPR requires that system owners provide an explanation. However, the database does not have automatic controls to preclude incorrect reporting, such as failure to respond to a trigger question.

Reporting

DoD Components did not accurately report information in DITPR. The DITPR Guidance reiterates the requirements of the E-Government Act by requiring that system owners conduct PIAs for any new or significantly altered IT system that collects, maintains, or disseminates information in identifiable form from or about members of the public. ASD(NII)/DoD CIO required for the first time that system owners complete PIA data elements in DITPR by March 1, 2006, and Privacy Act data elements by July 1, 2006. Additionally, OMB Memorandum 06-20 of July 17, 2006, requires that agencies immediately provide

quarterly updates on privacy program metrics to OMB to support the President's Management Agenda scorecard.

Systems Reviewed. System owners for 7 of the 18 systems (39 percent) stated that the PIA information in DITPR was not correct. In addition, an IA manager for four Navy systems stated that she did not know if the information in DITPR was correct because she did not assess the systems to determine whether they contained personally identifiable information. However, based on the information in the briefings of the systems provided to us by the system owners, we determined that data for 10 of the 18 systems (56 percent) was incorrect. Many of the system owners stated that they were confused when reporting PIA information in DITPR because system owners were not familiar with PIA requirements and therefore could not determine if a PIA was required. See Appendix C for the 18 systems reviewed and those not correctly reported in DITPR.

Army. We reviewed three Army IT systems that were reported in DITPR as requiring a PIA. The system owners of two systems, however, subsequently determined that their DITPR entry was not correct. The system owners stated that DITPR should report that no PIA is required for the two systems because they did not contain public information in identifiable form; however, we determined that one system contained personally identifiable information on members of the public. According to the system owner, the system contained loan information for family members or associates of DoD personnel. The loan information gathered on family members and associates includes names and addresses. In addition, the system is undergoing a major modification, which creates a new privacy risk. Therefore, systems owners should have conducted a PIA on the system and reported in DITPR that the system required a PIA.

The system owner for the third system stated that the location completed a PIA and correctly reported in DITPR that a PIA was required. Based on discussions with the system owners for the three Army systems reviewed, we determined that the DITPR reporting for one of the three systems was not correct.

Navy. We reviewed six Navy IT systems. A system owner for one system completed a PIA and correctly reported in DITPR that a PIA was required. Another system owner reported in DITPR that a PIA was required because the system contained privacy protected information. However, the system had existed for several years and was not undergoing any additional development. Therefore, the system did not meet the requirement of "new or significantly altered" system requiring a PIA. DITPR did not identify the caveat. Accordingly, the system owner should not have listed in DITPR that the system required a PIA.

System owners for the remaining four systems reported in DITPR that a PIA was not required for three systems and was required for the fourth system. However, the system owners stated that they did not assess the systems to determine whether a PIA was required because they were not familiar with the PIA requirements. In June 2006, the Navy issued PIA guidance that requires systems with personally identifiable information on public and DoD personnel to conduct a PIA. Based on the new guidance, we determined that all four systems required a PIA because the systems contained personally identifiable information.

In addition, the IA manager stated that the systems met the PIA requirements because the systems were constantly being modified. Based on discussions with the system owners for the six Navy systems reviewed, we determined that the DITPR reporting for four of the six systems was not correct.

Air Force. We reviewed six Air Force IT systems. The DITPR reported that four of the six systems required a PIA. System owners for three of the six systems stated that DITPR was not correct when reporting that a PIA was required for those three systems. The system owner for the fourth system prepared a draft PIA and reported in DITPR that a PIA was required. System owners for the remaining two systems reported in DITPR that a PIA is not required; however, one of the two systems met the criteria for requiring a PIA and contained personally identifiable information. The system required a PIA because it was initiating a new electronic collection of information in identifiable form for the public. Also, the system contained the names, social security numbers, and addresses for family members of DoD personnel and contractors. Based on discussions with the system owners for the six Air Force systems reviewed, we determined that the DITPR reporting for four of the six systems was not correct.

Additionally, at one Air Force location visited, two officials in charge of updating DITPR stated that they did not know who reported in DITPR that a PIA was required for their system and did not recall seeing the PIA question before. The two officials also stated that they were not familiar with a PIA or the PIA requirements.

DoD Agencies. We reviewed three DoD agencies' IT systems. One DoD agency official stated that when DoD issued PIA Guidance, there was confusion about which systems required a PIA. System owners for two of the three systems reported in the DITPR that the system required a PIA. However, the system owner for one of the two systems subsequently determined that the entry in DITPR, which identified that a PIA was required, was not correct. The official stated that the reason the system did not require a PIA was because the system is a National Security System and exempt from conducting a PIA. The system owner for the third system stated that the information in DITPR was correct, which stated that a PIA was not required. Based on discussions with the system owners for the three Defense agency systems reviewed, we determined that the DITPR reporting for one of the three systems was not correct.

DoD Component system owners should consult DoD PIA or Component implementing guidance when performing a PIA for systems containing personally identifiable information. Component PIA officials should ensure that all levels within their Component are aware of the DoD PIA and the Component's implementing guidance. System owners also need to verify that PIA information reported in DITPR is accurate, and Component PIA and privacy officials need to establish effective internal controls to verify reporting accuracy to provide OMB and Congress with an accurate reporting on the status of DoD information systems.

PIA Information in DITPR. The DITPR reporting on whether systems required a PIA fluctuated greatly. On February 13, 2006, DITPR identified that 188 DoD systems required a PIA; on August 3, 2006, 299 systems required a PIA; and on

September 5, 2006, DITPR reported that 198 systems required a PIA. As of September 8, 2006, DoD Components did not report in DITPR whether a PIA was required for 1,367 systems, which included 1,185 Army systems, 91 Navy systems, and 27 Air Force systems. ASD(NII)/DoD CIO officials stated that the information in DITPR variedly greatly because DITPR was implemented in phases.

Submitting PIAs. On February 14, 2006, the DoD PIA official stated that the DoD Components submitted only 19 approved PIAs to the DoD PIA office. On August 29, 2006, we asked whether the Components submitted additional PIAs to the DoD PIA office since February 2006. The Director of the office responsible for the DoD PIA Program stated that the job position designated to collect and post PIAs to the ASD(NII)/DoD CIO Web site was vacant. The DoD PIA official who was in place in February left in May and has not been replaced. The Director did not know how many additional PIAs the DoD Components submitted to the DoD PIA office. However, the DoD Components reported in DITPR, as of September 5, 2006, that they submitted 36 PIAs to OMB.

Validation of Information

Naval Postgraduate School Reporting. During interviews with the system owners for the 18 systems reviewed, we identified that other security data elements for 4 of the 18 systems in DITPR were not correct. The DITPR Guidance requires that system owners report whether a system requires certification and accreditation. A "yes" response to the question requires that the system owner complete the FISMA information in DITPR. The system owner must identify, as part of those questions, the accreditation method used for certifying and accrediting the system. The method could include the DoD Information Technology Security Certification and Accreditation Process, the DoD Information Assurance Certification and Accreditation Process, or the process used for intelligence systems.

System owners at the Naval Postgraduate School reported in DITPR that four systems had been certified and accredited when they were not. According to the IA manager, three of the four systems had been operational for 5 years, and the fourth system for 2 years. The IA manager stated that the systems were not certified and accredited because the certification and accreditation process was "too expensive and takes too long." The following are the four systems operating with no certification or accreditation:

- Departmental Online Reporting System;
- Electronic Time and Attendance Certification System;
- Management Information System; and the
- Python Education Management System.

Before we left the audit site, the IA manager provided memorandums, signed by the Designating Approving Authority, granting the four systems an interim authority to operate on May 10, 2006. The IA manager stated that the length of time the systems had been in operation and the Designated Approving Authority's familiarity with the four systems made granting the interim authority to operate appropriate. According to the IA manager, the interim authorities to operate were not based on security documentation or testing required for the system but on the Designated Approving Authority's knowledge of the system's performance.

The IA manager stated that the System Security Authorization Agreement—which documents the actions, decisions, security requirements, and the level of effort needed to certify and accredit any information system—will be prepared by the end of May 2007. The IA manager stated that once the System Security Authorization Agreements are complete, the Designated Approving Authority would grant the four systems an authority to operate.

As of June 2006, the Naval Postgraduate School reported in DITPR that three systems were accredited on May 10, 2006 and one system on May 31, 2006, in accordance with the DoD Information Technology Security Certification and Accreditation Process, and granted an authority to operate. DITPR also reported that accreditation would expire on May 10, 2009 and May 31, 2009, respectively. DITPR should report that the four systems have no authority to operate and that the accreditation vehicle element in DITPR did not apply because none was used.

The IA manager's methodology for granting a system approval to operate without being certified and accredited is flawed. DoD policy requires that a specific process be followed prior to granting a system authority to operate. One cannot base the decision to certify and accredit on the length of time a system has been in operation or whether the Designated Approving Authority is familiar with the system when granting the interim authority to operate.

Until the IA manager prepares the required documentation and appropriately tests the IA controls identified for the Departmental Online Reporting System, the Electronic Time and Attendance Certification System, the Management Information System, and the Python Education Management System, the Naval Postgraduate School should report to the Navy CIO and the DoD CIO that the systems are not certified and accredited. The IA manager should immediately certify and accredit the systems in accordance with DoD policy and develop a plan of action and milestones for how and when the certification and accreditation will be completed. Additionally, the Designated Approving Authority should not grant any authority to operate until the Certifying Authority certifies the system to operate in an environment that warrants an acceptable risk that the system's information is protected to the highest level required.

Validation of DITPR Information. Component CIOs did not validate the system information reported in DITPR. The DITPR guidance states that the Components and Component CIO are responsible for the completeness and accuracy of the information in DITPR. The guidance requires that a Component CIO certify in writing that he or she has complied with FISMA, PIA, and privacy

requirements. The DITPR guidance states that to have complete and authoritative data, the Component CIO should implement automated controls, revise internal business processes, and establish tracking mechanisms. At a minimum, Component CIOs should update and maintain their Components' input to DITPR quarterly. However, the guidance recommends that the CIO change from updating each quarterly to updating every time the information changes.

The CIOs for the Army, Navy, Air Force, and Defense Threat Reduction Agency did not correctly report in DITPR PIA information for 10 of 18 systems reviewed. Specifically, the Army did not correctly report PIA information in DITPR for one system, the Navy for four systems, the Air Force for four systems, and the DoD agencies for one system. Additionally, the Navy CIO did not validate the accuracy of information reported for the certification and accreditation status of four systems. Before executing written certifications, CIOs need to implement controls to correct PIA and related information in DITPR.

Prior Reporting

DoD Inspector General Report No. D-2006-042, "Security Status for Systems Reported in DoD Information Technology Databases," December 30, 2005, identifies that IT system information maintained in DITPR, previously known as the IT Registry, was unreliable. The report cites that the database was not reliable because the DoD CIO and Chief Financial Officer communities failed to enact sufficient controls ensuring the accuracy and consistency of Component system data. Additionally, the report identifies that ASD(NII)/DoD CIO did not enact sufficient controls that would ensure the accuracy of information in DITPR. Report No. D-2006-042 states that the DoD FISMA Report to OMB and Congress was based on system data that were uncertified by DoD Components and that OSD had no other internal control mechanism for validating the data that OSD, OMB, and Congress used for management purposes. The report concluded that the incorrect, inaccurate, and incomplete information in DITPR diminishes the usefulness of the database for management oversight. The report also concludes that unless DoD management develops and enforces effective internal quality assurance controls over Component-controlled data in DITPR, the situation will continue.

We recommended in DoD Inspector General Report No. D-2006-042 that ASD(NII)/DoD CIO advise OMB and the Congress that DoD did not have viable internal controls over the accuracy of data it is reporting on the security of its IT systems and investments and caveat all reports based on data drawn from unreliable databases, such as the IT Registry/DITPR and the Information Technology Management Application/Select Native Programming – Information Technology until effective internal controls are in place for at least one full year reporting cycle. The report also recommends that the ASD(NII)/DoD CIO develop internal controls other than Component CIO and Chief Financial Officer certifications, report the discrepancies between DoD databases as a material control weakness, and develop a Plan of Action and Milestones to track and correct deficient conditions. Until such time as the ASD(NII)/DoD CIO

effectively implements those recommendations, the information from DITPR generated in reports to OMB and Congress will remain unreliable.

The inaccurate PIA information and the Naval Postgraduate Schools misreporting of at least four systems in DITPR compounds the fact that the information in the DoD FISMA Report to OMB and Congress is unreliable. Unreliable information reported in the DITPR jeopardizes the efficient and effective management of IT systems and potentially compromises protection of personal information. The misreporting further demonstrates the need for ASD(NII)/DoD CIO to develop and enforce effective internal quality assurance controls to ensure accuracy of the DITPR information.

Conclusion

Component CIOs did not report accurate information in DITPR to the Office of the Secretary of Defense, OMB, and the Congress. As a result, the Office of the Secretary of Defense, OMB, and the Congress are making management and budgetary decisions based on unreliable reports generated from DITPR-the sole DoD-wide data repository for information at the system level for the status of DoD information systems. System owners should complete PIAs when required to guarantee that safeguards are in place to protect the public's personal information and limit risks. Completed PIAs are not being provided to the DoD CIO as required and the DoD CIO does not have an individual in place to track PIAs. The accreditation status for Navy systems puts information on those systems at risk.

ASD(NII)/DoD CIO and DoD Components must establish effective internal controls to verify that the information in DITPR is accurate. Previous DoD Inspector General audit reports identified inconsistencies and inaccuracies of the information being reported in DITPR. This persistent problem further demonstrates the need for ASD(NII)/DoD CIO to develop and enforce effective internal quality assurance controls to ensure accuracy of the DITPR information.

Recommendations, Management Comments, and Audit Response

C.1. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer:

a. Establish effective internal controls for DITPR; and

Management Comments. The ASD(NII)/DoD CIO concurred with the recommendation. Annual DITPR guidance has institutionalized a data quality improvement program with specific milestones. Data quality results are emphasized and reported at monthly meetings of the Technical Solutions Integrated Product Team and at bimonthly DITPR In-Process Reviews. The IT Management Data Community of Interest has been established to begin building a

netcentric capability for publishing and subscribing to all authoritative and complete DITPR data. Components will ensure that data they submit are complete and authoritative through a Verification and Validation study. The process should ensure that DITPR data elements across the Department are populated and traceable to complete and authoritative data once fully implemented.

Audit Response. Management comments are partially responsive to the recommendation. Although the proposed management corrective action is responsive to the intent of the recommendation, ASD(NII)/DoD CIO did not provide an estimated completion date for the corrective action as required by DoD Directive 7650.3, "Follow-up on General Accounting Office (GAO), DoD Inspector General (DoD IG), and Internal Audit Reports," June 3, 2004; Certified current as of October 18, 2006. We request that ASD(NII)/DoD CIO provide the proposed completion date.

b. Appoint an official who will manage and track approved Privacy Impact Assessments sent to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.

Management Comments. Management concurred with the recommendation. ASD(NII)/DoD CIO, Director of Management Services is assigned to manage and track PIAs.

Audit Response. ASD(NII)/DoD CIO comments were responsive to the recommendation; therefore, no further comments are required.

C.2. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer require that DoD Component Chief Information Officers:

a. Evaluate the Component inventory of systems in the DoD Information Technology Portfolio Repository to determine whether the systems contain personally identifiable information to include information on DoD personnel;

Management Comments. ASD(NII)/DoD CIO concurred with the recommendation. Management and the Component CIOs are evaluating systems that contain personally identifiable information.

Audit Response. The ASD(NII)/DoD CIO comments are partially responsive to the recommendation. Although proposed management corrective action is responsive to the intent of the recommendation, the ASD(NII)/DoD CIO did not provide an estimated completion date for the corrective action as required by DoD Directive 7650.3. We request that ASD(NII)/DoD CIO provide the proposed completion date.

b. Validate that the Privacy Impact Assessment as well as security status information reported in the DoD Information Technology Portfolio Repository for the program offices is accurate before certifying to the DoD Chief Information Office that the information is correct; and

Management Comments. The ASD(NII)/DoD CIO concurred with the recommendation. The revised PIA guidance and annual DITPR guidance will emphasize the importance of validating entries into DITPR and certifying that the information is correct. Reviews of the blank responses to the PIA trigger question and follow-ups with major Components to identify inconsistencies are being conducted. This data quality effort will continue until inconsistencies found in DITPR are corrected. A PIA and Privacy working group meeting is planned for late March 2007 to provide awareness training and guidance.

Audit Response. The ASD(NII)/DoD CIO comments are responsive to the recommendation; therefore, no further comments are required.

c. Implement automated controls, revise internal business processes, and establish tracking mechanisms that will provide complete and accurate information to the DoD Information Technology Portfolio Repository.

Management Comments. Management concurred with the recommendation. Reference Recommendation C.1.a.

Audit Response. The ASD(NII)/DoD CIO comments are partially responsive to the recommendation. Although management's proposed corrective actions are responsive to the intent of the recommendation, ASD(NII)/DoD CIO did not provide an estimated completion date for the corrective action as required by DoD Directive 7650.3. We request that ASD(NII)/DoD CIO provide the proposed completion date.

C.3. We recommend that the Chief Information Officer, Naval Postgraduate School:

a. Immediately begin efforts to certify and accredit the Reporting System, the Electronic Time and Attendance Certification System, the Management Information System, and the Python Education Management System in accordance with DoD policy.

Management Comments. The Naval Postgraduate School concurred with the recommendation. Management has begun the process of the DoD IT Security Certification and Accreditation Process for all four systems. Once completed, the System Security Authorization Agreement for each system will be submitted to Naval Network Warfare Command, Operational Designated Approval Authority for Approval to Operate. The estimated completion of this task is December 31, 2007.

Audit Response. Naval Postgraduate School comments were responsive to the recommendation; therefore, no further comments are required.

b. Report to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer; the Chief Information Officer, Department of the Navy; and in the DoD Information Technology Portfolio Repository that the Departmental Online Reporting System, the Electronic Time and Attendance Certification System, the

Management Information System, and the Python Education Management System are not certified or accredited.

Management Comments. The Naval Postgraduate School concurred with the recommendation. Management is working with the Department of Navy CIO office to accurately reflect the certification and accreditation status in the DITPR - Department of Navy. The estimated completion of this task is December 31, 2007.

Audit Response. The Naval Postgraduate School comments were responsive to the recommendation; therefore, no further comments are required.

c. Require that the Designated Approving Authority for the Departmental Online Reporting System, the Electronic Time and Attendance Certification System, the Management Information System, and the Python Education Management System not grant any authority to operate until the system owners certify the systems to operate in an environment that warrants an acceptable risk that the system's information is protected to the highest level possible.

Management Comments. Management concurred with the recommendation. The Naval Postgraduate School has completed the evaluation of the IA controls, the minimum security checklist for each system, the local residual risk assessment, and the risk statement. The Naval Postgraduate School, system owner, has confirmed the appropriate security protections are in place for the systems to process sensitive unclassified information. A Security Test and Evaluation is planned as part of the certification and accreditation process this year. The estimated completion of this task is December 31, 2007.

Audit Response. The Naval Postgraduate School comments were responsive to the recommendation; therefore, no further comments are required.

Appendix A. Scope and Methodology

Privacy Impact Assessments. We queried DITPR to identify the Components who were reporting that a PIA was or was not required for one or more of their systems. On February 13, 2006, 188 systems were identified in DITPR as requiring a PIA. We judgmentally selected 10 systems for review, 3 Army, 3 Navy, 2 Air Force, 1 TRICARE Management Activity, and 1 Defense Threat Reduction Agency. We also selected two systems, one Air Force and one Washington Headquarters Service system, that were reported in DITPR as not requiring a PIA.

We visited the Privacy and CIO offices for the Departments of the Army, the Navy, and the Air Force, the Defense Threat Reduction Agency, the Washington Headquarters Service, and the TRICARE Management Activity and the following 12 program offices responsible for the security of the systems selected for review. We reviewed whether system owners were correctly assessing whether a system required a PIA, reporting accurate PIA information in DITPR, and submitting PIAs to ASD(NII)/DoD CIO. We also reviewed whether the Components posted PIAs to their public Web sites.

- Army Criminal Investigative Command, Fort Belvoir Army Base, Fort Belvoir, Virginia
- Army Office of the General Council, Arlington, Virginia
- Army Corps of Engineers Finance Center, Millington, Tennessee and the Corps of Engineers Program Office, Huntsville, Alabama
- Naval Criminal Investigative Service, Washington Navy Yard, Washington, D.C.
- Navy Office of the Judge Advocate General, Washington Navy Yard, Washington, D.C.
- Naval Postgraduate School, Monterey, California
- Air Force Reserve Command, Robins Air Force Base, Georgia
- Office of Special Investigations, Andrews Air Force Base, Maryland
- Air Force Air Mobility Command, Scott Air Force Base, Illinois
- Defense Threat Reduction Agency, Fort Belvoir Army Base, Fort Belvoir, Virginia
- TRICARE Management Activity, Falls Church, Virginia
- Washington Headquarters Service, Arlington, Virginia

During our visits to the 12 program offices, we determined that the Navy and Air Force offices owned 6 additional systems. We reviewed 3 Navy and 3 Air Force systems at these locations. We did not select additional systems for the Army because the offices visited did not own any additional systems to review. See Appendix B for the 18 systems selected for review.

We evaluated the PIA program based on the requirements in the E-Government Act, OMB Memorandums 03-22 and 06-20, the DoD PIA Guidance, the FY06 DITPR Guidance, Army Regulation 340-21, SECNAV Instruction 5211.5E, and Air Force Instruction 33-332. The policy and guidance reviewed were dated from July 1985 through May 2006.

We conducted interviews with officials from ASD(NII)/DoD CIO responsible for the DoD PIA Program; Component-level CIOs, Component-level Privacy, PIA, and FOIA officials; and Privacy, PIA, and FOIA officials at the program offices.

DoD Privacy Program. At the 12 PIA program offices visited, we also met with privacy program officials to assess compliance with the DoD Privacy Program. Specifically, we reviewed systems of records in electronic and paper-based form, systems notices reported in the Federal Registry, privacy training programs, DoD and non-DoD forms containing personally identifiable information, and privacy staffing requirements at each office. We also reviewed personnel folders at the locations to determine whether Privacy Act statements were included on forms containing personally protected information, filed in a system of records, and retrieved by personal identifier.

We interviewed officials and obtained documentation from ASD(NII)/DoD CIO, the Defense Privacy Office, the Department of the Army CIO, Department of the Army FOIA/Privacy Act office, Army Corps of Engineers Headquarters, Secretary of the Navy Chief of Naval Operations FOIA office, Navy CIO, and Secretary of the Air Force Warfighting Integration and CIO.

We evaluated the DoD Privacy Program based on the requirements of the Privacy Act of 1974, DoD Directive 5400.11, DoD Regulation 5400.11-R, and OMB Memorandum M-06-15. The policy and guidance reviewed were dated from September 1974 through May 2006.

We performed this audit from January through December 2006 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Government Accountability Office High-Risk Area. GAO identified several high-risk areas in DoD. This report provides coverage of the Protecting the Federal Government's Information-Sharing Mechanisms and the Nation's Critical Infrastructures high-risk area.

Prior Coverage

During the last 5 years, the GAO and the DoD Inspector General issued three reports discussing the Privacy Act and PIAs. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Testimony GAO 06-77T, "Privacy, Key Challenges Facing Federal Agencies," May 17, 2006

DoD IG

DoD IG Report D-2004-033, "Terrorism Information Awareness Program," December 12, 2003

DoD IG Report D-2006-042, "Security Status for Systems Reported in DoD Information Technology Database," December 30, 2005

Appendix B. Forms Without Privacy Act Statements

We identified the following forms in a system of records that did not contain a Privacy Act statement:

- Department of the Army Form, "Certificate of Clearance and/or Security Determination"
- Department of the Army Form 1256, "Incentive Award Nomination and Approval"
- Department of the Army Form 7223, "Base System Civilian Evaluation Report"
- DD Form 214, "Certificate of Release or Discharge from Active Duty"
- Form PD-21 "Application Forms in the Distance Learning Product Development for the 21st Century"
- Form W-4, "Employee's Withholding Allowance Certificate"
- Form 7311, "Withholding Certificate for Local Taxes"
- Form 50271-101m, "Conversation Record"
- Memorandum Form CICG SC 380-67, "Notice of Intention to Hire"
- Memorandum Form CISP PE 690, "Emergency Contact"
- Optional Form B 873, "Position Description - D.C."
- Standard Form 7-B, "Request for Estimated Earnings During Military Service"
- Standard Form 50-B, "Notification of Personnel Action"
- Standard Form 1199A, "Direct Deposit"
- Standard Form 2817, "Life Insurance Election"

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense for Networks & Information Integration/DoD Chief Information Officer
Assistant Secretary of Defense (Health Affairs)
Director of Administration and Management
Director, Program Analysis and Evaluation

Department of the Army

Administrative Assistant to the Secretary of the Army
Auditor General, Department of the Army
Chief Information Officer, Department of the Army
Auditor General, US Army Corps of Engineers

Department of the Navy

Assistant Secretary of the Navy (Manpower and Reserve Affairs)
Naval Inspector General
Auditor General, Department of the Navy
Chief Information Officer, Department of Navy
President, Naval Postgraduate School

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Chief Information Officer, Department of the Air Force

Combatant Command

Inspector General, U.S. Joint Forces Command

DoD CIO Response to DoD Office of Inspector General (OIG) Draft Audit Report, "DoD Privacy Program and Privacy Impact Assessments" (Project No. D2006-D00AL-0087.000)

Section B. DoD OIG Privacy Impact Assessment (PIA) Recommendations

OIG Recommendation B.1. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, in coordination with the Director of Administration and Management, Office of the Secretary of Defense/DoD Senior Privacy Official:

a. Determine the most appropriate management structure for overseeing a Department-level Privacy and PIA program in accordance with the requirements of the E-Government Act of 2002 and Office of Management and Budget Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003, and subsequent Office of Management and Budget guidance for Privacy Impact Assessments and protection of personally identifiable information

Response: Concur. After review of the current management structure, a decision to keep the current management structure appears to be most appropriate. The Director, Defense Privacy Officer, Office of Director, Administration and Management (DA&M) and the Office of the DoD CIO work closely on OMB requirements concerning protecting personally identifiable information and privacy impact assessments.

The Director, Administration and Management, Office of the Secretary of Defense, is the designated DoD Senior Privacy Officer and responsible for privacy policy. The DoD Chief Information Officer responsibilities include but are not limited to information resources management, information systems, and performance of the duties and fulfillment of the responsibilities associated with information security and other matters under section 3544 of Title 44, United States Code.

b. Revise the charters of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Director of Administration and Management, Office of the Secretary of Defense/DoD Senior Privacy Official to reflect the conclusions reached under Recommendation B.1.a.

Response: NA. The current missions as recorded in DoD policies and regulations are appropriate.

c. Revise Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance," October 28, 2005, to reflect actions taken in accordance with Recommendations B.1.a. and B.1.b. and to:

Attachment (1)

DoD CIO Response to DoD Office of Inspector General (OIG) Draft Audit Report, "DoD Privacy Program and Privacy Impact Assessments" (Project No. D2006-D000AL-0087.000)

(1) Require that implementing guidance for the DoD Components' revised memorandum be reviewed and approved by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and issued within 60 days of publication of the revised Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer memorandum;

Response: Concur. The Office of the DoD CIO recommends 120 days instead of 60 days for the Components to issue their implementing guidance.

(2) Require that all DoD Components forward PIAs to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer for review and approval;

Response: Partially Concur. The Component CIOs are the subject matter experts to review and approve their system PIA. The Components will be required to submit their PIAs to the Office of the DoD CIO after approved at the Component level for submission to the Office of Management and Budget (OMB). The revised DoD PIA guidance will incorporate this requirement in fourth Quarter FY07.

(3) Require that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, rather than Component Chief Information Officers be responsible for submitting approved privacy impact assessments to the Office of Management and Budget;

Response: Concur. The revised DoD PIA guidance will incorporate this requirement.

(4) Require that all personally identifiable data for DoD employees be afforded the same level of assessment and protection provided to data for the general public;

Response: Concur. The revised DoD PIA guidance will incorporate this recommendation. Of note, DoD CIO Policy Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006, directed Components to ensure that all PII not explicitly cleared for public release be protected according to Confidentiality Level Sensitive, as established in DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

(5) Clarify how the privacy impact assessment request link on the Web site of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer is responsive to the requirement of the E-Government Act to make privacy impact assessments publicly available;

Response: Concur. Currently, each Component maintains a repository of its PIAs. They are required to be posted at a central location on the Component's public website until the system is terminated. The DoD CIO website maintains a "PIA Request" link to respond to public requests regarding DoD IT systems containing information in identifiable form. In the future, the DoD

CIO PIA website will display a link to each Components PIA website listing all PIAs. Estimated completion date for this task is in fourth Quarter FY07.

(6) Specify the target audience and nature of training that DoD components are required to provide for privacy impact assessments.

Response: Concur. The nature of the training is to understand the requirements to do PIAs and the DoD PIA guidance. The Office of the CIO annually briefs the DoD resource managers on the PIA requirements for the major IT systems reported in the Exhibit 300s. In the near future (by July 31, 2007), the Office of the DoD CIO will review the curriculums at Defense Acquisition University and Information Resources Management College to ensure content is captured in their courses. In addition, we are in the process of adding PIA training content in the DISA Information Assurance training program, which is distributed DoD-wide. Expected completion July 31, 2007.

B.2. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer require that DoD Component CIOs:

a. Disseminate Office of Management and Budget Memorandum 03-22 and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer October 28, 2005, privacy impact assessment guidance to all Component information technology system owners to assist them in conducting required privacy impact assessments, pending receipt of revised DoD and DoD Component guidance;

Response: Concur. Estimated completion date for this task is May 31, 2007.

b. Advise subordinate Component Chief Information Officers and privacy officers that personally identifiable data for DoD employees should be afforded the same level of assessment and protection offered to similar data from the general public.

Response: Concur. The revised DoD PIA guidance will incorporate this recommendation.

Section C. Reporting in the DoD Information Technology Portfolio Repository (DITPR), DoD OIG Recommendations.

C.1. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer:

a. Establish effective internal controls for DITPR;

DoD CIO Response to DoD Office of Inspector General (OIG) Draft Audit Report, "DoD Privacy Program and Privacy Impact Assessments" (Project No. D2006-D000AL-0087.000)

Response: Concur. To establish and police effective internal controls, annual DITPR guidance has institutionalized a data quality improvement program with specific improvement milestones. Data quality results are emphasized and reported at each monthly Technical Solutions IPT meeting and at the bi-monthly DITPR IPR. In addition, the DoD CIO has established an IT Management Data Community of Interest (COI). This COI has begun the process of building a Net-Centric capability for publishing and subscribing to all authoritative and complete DITPR data. As part of this process, each Component entering data into DITPR will document, in a detailed Verification and Validation study, how they are assured that the data they are submitting to DITPR is complete and authoritative. When fully implemented, the processes established by the COI should ensure that DITPR data elements across the Department are populated and traceable to complete and authoritative data.

b. Appoint an official who will manage and track approved privacy impact assessments sent to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.

Response: Concur. The DoD CIO, Director of Management Services is assigned to manage and track privacy impact assessments and to work closely with the Director, Defense Privacy Officer, Office of Director, Administration and Management. **Action completed.** Recommend close out.

C.2. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer require that DoD Component Chief Information Officers:

a. Evaluate the Component inventory of systems in the DoD Information Technology Portfolio Repository to determine whether the systems contain personally identifiable information to include information on DoD personnel;

Response: Concur. The Office of the DoD CIO and the Component CIOs are in the process of evaluating which systems contain PII in their systems.

b. Validate that the privacy impact assessment as well as security status information reported in the DoD Information Technology Portfolio Repository for the program offices is accurate before certifying to the DoD Chief Information Office that the information is correct; and

Response: Concur. The revised PIA guidance and annual DITPR guidance will emphasize the importance of validating entries into DITPR and certifying that the information is correct. Since November 1, 2006, the Office of the DoD CIO PIA POC has been reviewing the validity of the PIA data and corresponding with the Components to correct their information. Over the last 4 months, the Component PIA POCs have reduced the number of blank PIA trigger answers from approximately 800 in September 2006 to 179 blanks on February 27, 2007. In addition, follow-ups are being conducted with the major Components to identify inconsistencies in their data.

This data quality effort will continue until the inconsistencies found in the DITPR are corrected. On February 16, 2007, the Office of the DoD CIO held a meeting with the major Components to discuss PIAs and issues. A PIA and Privacy working group meeting will be held in late March 2007 to provide awareness training and guidance. The DoD OIG representatives will be invited to this meeting and future meetings of this working group.

c. Implement automated controls, revise internal business processes, and establish tracking mechanisms that will provide complete and accurate information to the DoD Information Technology Portfolio Repository.

Response: Concur. The DoD CIO has established an IT Management Data COI. This COI has begun the process of building a Net-Centric capability for publishing and subscribing to all authoritative and complete DITPR data. As part of this process, each Component entering data into DITPR will document, in a detailed Verification and Validation study, how they are assured that the data they are submitting to DITPPR is complete and authoritative. When fully implemented, the processes established by the COI should ensure that DITPR data elements across the Department are populated and traceable to complete and authoritative data.

Director of Administration and Management Comments

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

MAR 14 2007

MEMORANDUM FOR THE INSPECTOR GENERAL, DOD

SUBJECT: Report on Audit of DoD Privacy Program and Privacy Impact Assessments (Project No. D2006-D000AL-0087.000)

I appreciate the opportunity to review and comment on your draft audit report of the DoD Privacy Program.

Except as otherwise noted in the attached comments, I generally concur with your Findings but not with your recommendations. As discussed in the attachment, the current or soon to be revised DoDD 5400.11 and DoD 5400.11-R appear to provide the necessary and appropriate guidance to the Military Departments and the DoD Components. However, I also am directing that a review of the DoD Privacy Program be conducted where, among other objectives, the effectiveness of the decentralized management approach to Privacy will be assessed, to include what personnel and resources may be required to strengthen the current program. The target date for completion of the review is in the fourth Quarter, FY 2007.

Your audit, however, identifies a systemic problem that continues to impact the DoD Privacy Program, i.e., the failure of many in the DoD workforce to be cognizant of the applicable statutory and regulatory requirements for Privacy. As you would agree, absent a workforce that is sensitive and responsive to program requirements and demands, there will be failures. And while the failures are attributable to ignorance of the rules and regulations, and not to acts of malfeasance, the fact remains that the failures frustrate key objectives sought by Congress in the Privacy Act of 1974.

I firmly believe that a viable training program, where individuals who interact with privacy protected information are made aware, and are subsequently reminded, of their reporting and safeguarding responsibilities under the law and implementing DoD/Component regulation, is the key to overcoming the present program deficiencies. As your report points out, a framework for Privacy training now exists in DoD 5400.11-R. The problem is that implementation of the training requirements is not uniform across the Components, principally because time and resource constraints impact a Component's ability to provide the needed training. But as you also have discovered during the audit, the Components are making use of technology, i.e., web-based, to reach their target audiences and to provide such training. As such training is expanded and fine-tuned, it is anticipated that workforce awareness of program requirements and demands will increase and that program vulnerabilities will decline.

Michael B. Donley
DoD Senior Privacy Official

Attachment:
As stated

Final Report Reference

DoDIG Project No. D2006-D000AL-0087.000

"Report on Audit of DoD Privacy Program and Privacy Impact Assessments"

DoD Senior Privacy Official Comments

Page 4.

Finding. The report states that program failures occurred, in part, because the DoD Privacy Office (DPO) has not established oversight mechanisms for effective Program execution.

The report does not acknowledge that DPO has a number of mechanisms in place, similar to those used by the Office of Management and Budget in its oversight role for Federal Privacy, that permits DPO to oversee the Component Privacy Programs. First, it has a dedicated technical channel with Component Privacy officials that provides DPO not only insight as to what is occurring in the Component but permits the Component to surface problems that they are encountering. Second, DPO exercises oversight in its role as a reviewing and approval authority for Privacy Act system of records notices. The review process provides a window into how the Components are complying with the requirements of the Act. Third, DPO exercises oversight via the Federal Information Security and Management Agency (FISMA) Privacy Report, a report card on how agencies are complying with Federal privacy mandates. As part of the Department's report to OMB, DPO prepares a narrative statement based, in part, on input provided by the DoD Components. In effect, the Components are tasked to assess their programs. The resulting input provides a window into how the Components are viewing their respective Privacy Programs. This input also provides DPO an opportunity to assess the current health of the Component's Program. And fourth, the DoDIG and Component IGs are a means, as evidenced by the instant audit, to exercise oversight, a means that, until now, has not been frequently utilized.

Page 6 and Appendix B.

Finding. The report identifies a number of Forms that did not include a Privacy Act Statement (PAS).

A review of each of the identified Forms was not conducted. However, Standard Form (SF) 2817 and the SF 1199A do contain a PAS. For the Form 2817, the location of the PAS is described at the top of page 1. For the Form 1199A, the PAS is set forth on the back of the Form under the heading ""Please Read This Carefully." And finally, SF 50-B does not require a PAS as information is not being collected directly from the individual.

Pages 11-16

Pages 10-11.

Recommendation a.(1). Modify DoDD 5400.11 to require DoD Components to provide bi-annual certifications to the DPO for review that Program requirements, e.g., training, system of records notices, Privacy Act Statements, etc. are being implemented and followed.

The report acknowledges that current program requirements are set forth in DoDD 5400.11 and DoD 5400.11-R. The Components are now under an affirmative obligation to ensure that the Program mandates are met. In turn, the Components have promulgated privacy issuances that reaffirm the requirements set forth in the DoD issuances.

A biannual certification requirement will not remedy the deficiencies identified in the report nor will it significantly contribute to the DPO exercising oversight over the Component's programs. As the report makes clear, program execution is not due to the lack of guidance, but to the fact that Component personnel are not always aware of the guidance. These failings will persist until the workforce is sensitized to the demands and requirements of the program.

Component FISMA Privacy reporting is a much more effective tool for overseeing and reviewing Component compliance with program requirements.

Recommendation a.(2). Modify DoDD 5400.11 to require DoD Components to require that PASs are included on any DoD and non-DoD form used to collect identifiable information regardless of who provides the information.

The report points out that DoD 5400.11-R currently requires that Forms, whether DoD or not, contain a PAS if the information is being collected directly from the individual and is to be filed in a Privacy Act system of records.

Neither the Privacy Act nor the DoD guidance require that a PAS be provided by a third party who is furnishing information about an individual. Congressional intent was that information be collected to the greatest extent practicable from the individual and that when collecting such information that the individual is provided certain information so that he or she could make an informed decision whether or not the information should be furnished. Congress, however, recognized that this requirement may not be practical in all cases for financial or logistical reasons or because of other statutes. Such a case exists when supervisors or other administrative personnel enter information into a Privacy Act system of records based on information that is available to them. Such personnel are executing the duties of their offices and in order to properly discharge those duties, the information must be entered.

Recommendation a.(3). Modify DoDD 5400.11 to require that Privacy Officers receive management privacy training within 90 days of appointment and include the privacy training requirement in performance standards established by Privacy Officials.

It is agreed that, unless designated Privacy Officials are trained, their ability to execute a successful Privacy Program is impacted. DoD 5400.11-R, rather than DoDD 5400.11, will be changed to incorporate this specific requirement.

Incorporating a privacy training requirement into the performance standards of Privacy Officials possesses merit and warrants further study. This proposal will be evaluated as part of the DoD Privacy Program review.

Recommendation a.(4). Modify DoDD 5400.11 to require that individuals implementing privacy requirements and/or handling personal information receive appropriate specialized training and management training identified in DoD 5400.11-R.

The current DoD Regulation on Privacy provides guidance on such training. The revised Regulation, which is undergoing final review, has been expanded to provide additional guidance as well.

Recommendation a.(5). Modify DoDD 5400.11 to require annual Privacy Act Awareness training for all DoD employees that includes a certification for completion.

How often Privacy Awareness training should be offered and conducted is now at the discretion of the Components as they are in the best position of judging the need and frequency for such training.

The soon to be approved DoD Regulation on Privacy will provides that, insofar as personnel who interact with privacy protected information are concerned, Components shall conduct training as frequently as believed necessary so as to ensure that personnel are sensitive to the requirements of the Regulation. The Regulation further will provide that 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.

Recommendation b. Assess the DoD privacy program for staffing levels and resources required to enable Privacy officials to effectively fulfill their Privacy duties and recommend resource allocations to ensure a viable Privacy program.

It is agreed that Component staffing levels and resources should be assessed with a view of determining what can be done to enhance Program effectiveness. The Assessment will be conducted as part of the DoD Privacy Program review.

Recommendation c. Modify DoDD 5400.11 to require Component Privacy Officials , in coordination with the Component Chief Information Officers, support preparation of the certifications required in Recommendation a.

Unless a Component Chief Information Officer is responsible for the Component Privacy Program, the Component CIO will not have a direct role in a Component's Privacy Program.

This does not mean that the Component CIOs do not have a critical role to play regarding Privacy. They do. The CIO has primary responsibility for technical security of Component IT systems. In this area, it can be said that there is a "shared" responsibility between the Component Privacy Official and the Component CIO as the CIO responsibilities directly impact the Component's Privacy Program. In effect, the Component Privacy Official relies on the Component CIO to develop the appropriate technical safeguards that will safeguard personally identifiable information in IT systems, thereby permitting the Component to be in compliance with the Privacy Act and implementing DoD/Component authority.

Recommendation c.(1). Modify DoDD 5400.11 to require Component Privacy Officials, in coordination with the Component Chief Information Officers, to develop an authoritative inventory of Component systems of records containing personally identifiable information.

DoD 5400.11-R presently requires that DPO maintain an authoritative inventory of Component Privacy Act systems of records notices. The inventory, which is posted to the DPO web site at www.dod.mil/privacy/notices, contains the notices for 1,174 systems of records. The inventory covers automated (IT) systems, manual systems, and hybrid systems (part automated, part manual).

Recommendation c.(2). Modify DoDD 5400.11 to require Component Privacy Officials, in coordination with the Component Chief Information Officers, to prepare system notices for the inventory of system of records being maintained.

DoD 5400.11 presently imposes an affirmative obligation on DoD system managers to prepare promptly any required new, amended, or altered system notice for the system and to forward them to the Component Privacy Official for review when a system qualifies as a Privacy Act system of records,.

Recommendation c.(3). Modify DoDD 5400.11 to require Component Privacy Officials, in coordination with the Component Chief Information Officers, to oversee subordinate privacy programs by conducting privacy reviews and verifying that privacy training is being conducted at all required levels.

Component Privacy Official are currently required, incident to providing input for the FISMA Privacy Report, to review their Privacy Programs, to include assessing whether their training programs are ensuring that personnel are generally familiar with information privacy laws, regulations and policies and whether appropriate job-related training is being offered.

Naval Postgraduate School Comments

DEPARTMENT OF THE NAVY
NAVAL POSTGRADUATE SCHOOL
1 UNIVERSITY CIR
MONTEREY CA 93943-5000

IN REPLY REFER TO:
3000
Ser 00/018
2 Mar 07

From: President, Naval Postgraduate School
To: Department of the Navy - Chief Information Officer

Subj: DoDIG DRAFT OF A PROPOSED REPORT, DoD PRIVACY PROGRAM AND PRIVACY IMPACT ASSESSMENTS (PROJECT NO. D2006-D000AL-0087.000)

Ref: (a) DOD IG Memorandum of February 6, 2007
(b) DODIG Project No. D2006-D000AL-0087.000 Draft Report

Encl: (1) Management Comments to Recommendations

1. Per references (a) and (b) this is in response to subject draft report of 6 February 2007, provided to this office for review and comment. Upon review of the draft report, we concur with the findings made by the Office of Inspector General (OIG), Department of Defense (DoD). NPS has addressed all recommendations and have either implemented or are in the process of implementing them.

2. Please address any questions to Ms. Lynn Murch or Ms. Denise Ross, Command Evaluation, Tel: 831.656.2557/2751 or email lmurch@nps.edu/djross@nps.edu.

DAVID A. SMARSH
Chief of Staff

Enclosure (1)

**Management Response to DoD IG Draft Audit Report,
Project No. D2006-D000AL-0087.000, DoD Privacy Program
and Privacy Impact Assessments, dated 6 February 2007**

c. **Reporting in the DoD Information Technology Portfolio Repository.**

Recommendation C.3.a: Immediately begin efforts to certify and accredit the Reporting System, the Electronic Time and Attendance Certification System, the Management
Information System, and the Python Education Management System in accordance with DoD policy.

Management Comment: Concur. The four Naval Postgraduate School systems listed in the DITPR-DON, the Departmental Online Reporting System, the Electronic Time and Attendance Certification System, the Management Information System and the Python Education Management Systems have begun the process of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The following portions of the DITSCAP have been completed: the contingency plans have been written and tested, the DoD 8500.2 Information Assurance Controls that require annual review have been reviewed, the DoD 8510.1 Minimum Security Checklist has been completed and a residual risk assessment has been completed. We will conduct the Security Test and Evaluation and to complete the written documentation for the System Security Authorization Agreement (SSAA) on each system. The SSAA will then be submitted to NETWARCOM, Operational DAA for Approval to Operate (ATO).

Estimated Completion Date: The estimated date of completion is 31 Dec 07.

Recommendation C.3.b: Report to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer; the Chief Information Officer, Department of the Navy; and in the DoD Information Technology Portfolio Repository that the Departmental Online Reporting System, the Electronic Time and Attendance Certification System, the Management Information System, and the Python Education Management System are not certified or accredited.

Management Comment: Concur. The Naval Postgraduate School is currently working with the Department of Navy Chief Information Officer's office to accurately reflect the certification and accreditation status in the DoD Information Technology Portfolio Repository - Department of Navy.

Estimated Completion Date: The estimated date of completion is 31 Dec 07.

Recommendation C.3.c: Require that the Designated Approving Authority for the Departmental Online Reporting System, the Electronic Time and Attendance Certification System, the Management Information System, and the Python Education
Management System not grant any authority to operate until the system owners certify the systems to operate in an environment that warrants an acceptable risk that the system's information is protected to the highest level possible.

Management Comment: Concur. The Naval Postgraduate School has completed the evaluation of the information assurance controls, and the minimum security checklist for each system. The residual risk assessment has been done locally and the risk statement has been completed. The system owner, the Naval Postgraduate School, has confirmed the appropriate security protections

are in place for the systems to process sensitive unclassified information. Additionally, a Security Test and Evaluation is planned as part of the certification and accreditation process this year.

Estimated Completion Date: The estimated date of completion is 31 Dec 07.

Department of the Navy Comments

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

8 March 2007

From: Department of the Navy Chief Information Officer

To: Inspector General, Department of Defense
Audit Follow-up and GAO Affairs
400 Army Navy Drive
Arlington, VA 22202

Subj: DOD-IG PROJECT NO. D-2006-D000AL-0087.000, "REPORT ON AUDIT OF THE DOD PRIVACY PROGRAM AND PRIVACY IMPACT ASSESSMENTS" – RESPONSE TO DRAFT REPORT ISSUED 6 FEB 2007

Encl: (1) NAVPGSCOL ltr 3000 Ser 00/018 of 2 Mar 07

The above referenced audit report recommended revisions to the Department of the Navy's (DON) Privacy Program. The DON Chief Information Officer (CIO) concurs with the need to update the SECNAVINST 5211.5E in order to reflect changes in DON's management of its Privacy Program and affected policies and practices. Specifically, SECNAVINST 5211.5E is under review and will incorporate recommendations made by the Department of Defense Inspector General (DoD-IG) audit team, as appropriate. The DON will implement the Privacy Program requirements stipulated by the Office of Management and Budget (OMB) and the Department of Defense (DoD) to ensure the security of Personally Identifiable Information (PII) throughout the DON.

The DON agrees the ever-increasing threats to PII, through accelerated technological advances, increases vulnerability. Significantly, the substantial increase in identity theft reports necessitated additional financial, human, and equipment resources be devoted to the Privacy Program effort. Accordingly, the DON took the following actions in concert with the DON Privacy Act and Freedom of Information Act Office to reduce the threat and increase awareness for our personnel:

- Updated the DON's privacy web site, including identification of all approved Privacy Act Systems of Records.
- Reviewed approximately one-third of the DON's system inventory to ensure proper reporting.
- Listed all changes to systems and posted these changes to the DON's privacy web site.
- Developed and posted required privacy training materials on the DON's privacy web site.
- Issued the SECNAVINST 5211.5E in December 2005, which is currently being revised to ensure compliance with recent regulatory changes.
- Formed Privacy working groups to address best practices and improve DON policy and guidance.
- Designated one Full Time Equivalent (FTE) in the Information Assurance (IA) section of the DON CIO to focus on Privacy Impact Assessments (PIA) and coordinate activities with the DON Privacy Act and Freedom of Information Act Office.

Subj: DOD-IG PROJECT NO. D-2006-D000AL-0087.000, "REPORT ON AUDIT OF THE DOD PRIVACY PROGRAM AND PRIVACY IMPACT ASSESSMENTS" – RESPONSE TO DRAFT REPORT ISSUED 6 FEB 2007

In an effort to coordinate its policies within the DON, the DON Deputy CIO (Marine Corps) reports that it is drafting policy for the:

- Initiation, processing, review, and submission of PIAs for information technology systems.
- Handling, maintaining, disposal, and training of personnel with regard to PII.
- Reporting of loss or possible compromise of PII.

The DON CIO confirms the specific recommendations provided in the audit regarding the Naval Postgraduate School were accepted and are being instituted. Enclosure (1) provides substantial details on actions being taken.

The DON has met the intent of the audit by committing additional resources, instituting appropriate changes to privacy policies and procedures, incorporating recommendations from several sources, and improving the Navy's and Marine Corps' management of PII. We appreciate the DoD-IG's efforts in support of the DON to improve the effectiveness of our Privacy Program.

John J. Lussier
(Acting)

Copy to:
NAVINSGEN (Attn: J. Gilbert)
CNO (N61)
CMC (C4)

Department of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

8 March 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

FROM: SAF/XC

SUBJECT: DoDIG Draft Audit Report, DoD Privacy Program and Privacy Impact Assessments, (Project No. D2006-D000AL-0087.000)

1. This is in reply to your memorandum requesting the Assistant Secretary of the Air Force (Financial Management and Comptroller) to provide Air Force comments on subject report.

2. I appreciate the opportunity to review and comment on your draft audit report of the DoD Privacy Program relative to the Air Force portion.

3. The Air Force concurs, without comment, to the DoDIG audit Findings/Recommendations associated with Section A, *Privacy Act Program*, and Section B, *Privacy Act Impact Assessments*.

4. The SAF/XC POC is Ms. Novella S. Hill, Air Force Privacy Act Officer, (703) 588-7855, novella.hill@pentagon.af.mil.

W. T. Lord

WILLIAM T. LORD, Maj Gen, USAF
Director, Information, Services and Integration
Office of Warfighting Integration and
Chief Information Officer

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Readiness and Operations Support prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Kathryn M. Truex
Karen J. Goff
Robert R. Johnson
Zachary M. Williams
Bryan T. Clark
Xavier R. Zayas