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

ADMINISTRATION AND
MANAGEMENT

APR 27 2007

MEMORANDUM FOR THE OFFICE OF MANAGEMENT AND BUDGET,
ATTN: KAREN EVANS

SUBJECT: Personally Identifiable Information

This responds to your email request of April 23, 2007, as updated by your email of April 25, asking that agency Senior Privacy Officials certify that (1) an agency has reviewed its use of SSNs and has adopted a plan to eliminate unnecessary usage of the number, (2) an agency has reviewed its policies and processes, and taken corrective action as appropriate, regarding the safeguarding of PII, and (3) that agencies have reminded their personnel of their specific responsibilities for safeguarding PII, the rules for acquisition and use, and the penalties for violations of the rules. Your request further asks that agencies (1) list weaknesses from all POA&M's that have slipped more than 30 days, (2) describe steps taken to publish a routine use as identified by the President's Identity Theft Task Force, (3) conduct a survey of their grant and loan programs, and (4) identify programs feeding information into the Federal Assistance Award Data System (FAADS).

The following information is provided in response to the above requests.

Agency SSN Review. In December 2006, OMB tasked agencies "to review their use of SSNs to determine whether such use can be eliminated, restricted, or concealed in agency business processes, systems and electronic forms."

The Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)) assumed responsibility for conducting the survey as it has principal responsibility for SSN policy within the Department because the SSN is used as the principal means for identifying DoD personnel and members of the greater DoD community. The survey was conducted and was provided OMB on March 26, 2007. However, it is my understanding that OMB submitted follow-up questions on April 19 and that efforts are now underway to acquire the additional information. It is anticipated that an updated report will be furnished in approximately two weeks.

Though I was not directly involved in the survey, I recognized that current Departmental privacy policies relating to the use of the SSN must be updated to reflect the outcomes sought by OMB and the President's Identity Theft Task Force in this area. Such policies have been incorporated into the DoD regulation on privacy, an issuance that I am about to approve. The new policy will mandate that, among other requirements, the "DoD Components shall continually review their use of the SSN to determine whether such use can be eliminated, restricted, or concealed in Component business

processes, system and paper and electronic forms" (see paragraph C2.1.2.7 of Attachment 1. Also see paragraph C2.1.2.6). The new requirements place an affirmative duty on the Components to determine whether initial or continued use of the SSN is warranted.

Additionally, OUSD(P&R) advises that it is currently developing a plan to identify unnecessary use of the SSNs and a course of action to eliminate or replace those SSNs identified as being unnecessary. It is estimated that it will take 6 – 12 months to complete the plan due to the magnitude of the task and the fact that DoD has global operations, the scope of SSN use across the DoD enterprise (including processes, systems, forms, etc.), the time required to evaluate SSN's use in each identified business application, identification of acceptable alternatives to the SSN which meets privacy and other criteria, and the development of cost impacts of removal/replacement of the SSN.

OUSD(P&R) further advises that the Departmental response to a Congressional tasking to provide the implications of removing the SSN from military identification cards (which serve as identification cards under the Geneva Conventions) is currently expected to be released next month. As this report will likely disclose the potential costs involved if the SSN is removed from the card, this may prove to be a measure of what the possible resource implications will be in executing the above plan.

Agency Review of PII Safeguarding Policies. In OMB Memorandum (M-06-15), dated May 22, 2006, OMB directed that agency Senior Privacy Officials "conduct a review of [their] policies and processes, and take corrective action as appropriate to ensure [agencies have] adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information."

As requested by OMB, the results of the study were to be included as part of the agency's 2006 FISMA Privacy Report. I am again furnishing an extract of the DoD report (Attachment 2) that addresses the study. Overall, the review disclosed that the agency had "adequate safeguards or, where not, actions are being initiated to either enhance the existing safeguards or to establish new safeguards."

DoD policies mandate that the appropriate administrative, technical, and physical security be established to assure that the confidentiality of the data is preserved and protected. Of special note is the fact that the DoD CIO rewrote the current policies on safeguarding PII, policies that are being incorporated into the DoD regulation on privacy.

Agency Employee Reminders on Safeguarding Information. In M-06-15 as well, OMB directed that agencies remind their employees within 30 days "of their specific responsibilities for safeguarding personally identifiable information, the rules for acquiring and using such information as well as the penalties for violating these rules." I am providing a copy of the DoD memorandum (Attachment 3) that was disseminated throughout the Department on this matter.

Though OMB did not seek a final report on agency efforts to notify all employees, it did seek a status report at one time on the percentage of employees notified and the

method of notification. At that time, most, but not all, of the DoD Components responded that they were disseminating the required information, primarily by electronic means (e.g., intranet postings, email, mandatory web-based training), believing it was the fastest means of reaching the broadest audience.

Given the size of DoD and the fact that we are engaged in a global war on terror, the actions taken by the Component to remind their personnel of their responsibilities in this area met the overall objective sought by the OMB.

POA&M Weaknesses. As requested, I also am providing the updated status of the DoD FISMA POA&M (Attachment 4).

Routine Use. The DoD has not taken any action to publish a routine use (RU) as contemplated by the President's Identify Theft Task Force as it was understood that the OMB was intending to incorporate implementing instructions on the RU into its draft guidance on Safeguarding PII. Therefore, publication was held in abeyance pending receipt of the OMB guidance in the event OMB made changes to the model RU. However, the Department is ready to publish the RU as crafted by the Task Force. The DoD will submit the required notice for publication and will forward the required Congressional and OMB reports NLT May 4, 2007. Depending upon the publication schedule of the Office of Federal Register, it can be anticipated that publication will occur within 7-10 days of the notice being sent. The RU will apply to all DoD Privacy Act systems of records, a listing of which is set forth at www.defenselink.mil/privacy/notices.

Grant and Loan Program Survey. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) will have the lead for conducting the required survey. The Department is still exploring how the survey can be conducted as it generally does not have centrally managed grants programs. Rather, programs are decentralized across numerous DoD Component awarding offices. Moreover, most of the Department's grants are awarded under programs in awarding offices that appropriately use various instruments, including grants, contracts, cooperative agreements and other financial assistance and acquisition transactions. This leads each awarding office to use for grants many of the same business processes and information systems that it uses for contracts, to the extent that doing so is consistent with the substantive distinctions between financial assistance and procurement. This sharing of awarding offices' processes and systems does not easily lend itself to a quick response to the proposed survey.

The Department has raised concerns about the present survey and the potential implications it raises insofar as the Privacy Act is concerned. We are hopeful that OMB will address our concerns and provide further guidance in this area.

The Department will establish a target date for completion once it determines what must be done in order to conduct the survey. It is possible that it may take significant

time and resources to complete the survey. If true, it is not anticipated that it will be finished in the near future.

FAADS. The USD(AT&L) also will have the lead in identifying programs providing information to the FAADS. After identification is made, my office as well as the Office of the DoD CIO will coordinate with the OUSD(AT&L) on matters involving a SORN or a PIA.

My point of contact for any questions relating to this memo is Vahan Moushegian, Jr., Director, Defense Privacy Office/703.607.29434/www.vahan.moushegian@osd.mil.

Michael B. Donley
DoD Senior Privacy Official

Attachments:
As stated

C2.1.2.6. Components shall ensure that the SSN is only collected when there is demonstrated need for collection. If collection is not essential for the purposes for which the record or records are being maintained, it should not be solicited.

C2.1.2.7. DoD Components shall continually review their use of the SSN to determine whether such use can be eliminated, restricted, or concealed in Component business processes, systems and paper and electronic forms. While use of the SSN may be essential for program integrity and national security when information about an individual is disclosed outside the DoD, it may not be as critical when the information is being used for internal Departmental purposes.

C2.1.3. Collecting Personal Information from Third Parties. When information being solicited is of an objective nature and is not subject to being altered, the information should first be collected from the individual. But, it may not be practicable to collect personal information first from the individual in all cases. Some examples of this are:

C2.1.3.1. Verification of information through third-party sources for security or employment suitability determinations;

C2.1.3.2. Seeking third-party opinions such as supervisor comments as to job knowledge, duty performance, or other opinion-type evaluations; and

C2.1.3.3. When obtaining information first from the individual may impede rather than advance an investigative inquiry into the actions of the individual.

C2.1.3.4. Contacting a third party at the request of the individual to furnish certain information, such as exact periods of employment, termination dates, copies of records, or similar information.

C2.1.4. Privacy Act Statements

C2.1.4.1. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act statement is required regardless of the medium used to collect the information (paper or electronic forms, personal interviews, telephonic interviews, or other methods). The Privacy Act statement consists of the elements set forth in subparagraph C2.1.4.2 of this Chapter. The statement enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any system of records. When soliciting SSNs for any purpose, see subparagraph C2.1.2.2 of this Chapter.

C2.1.4.2. The Privacy Act statement shall include:

C2.1.4.2.1. The Federal statute or Executive Order that authorizes collection of the requested information. See paragraph C1.1.4 of Chapter 1.

ATTACHMENT 1

uses of the information for that particular system. Though the DPO does not provide the DoDIG a copy of each notice, all DoD system notices are posted to the DPO web site (http://www.defenselink.mil/privacy), thereby giving the DoDIG, as well as others, to include the public, access as to how the Department uses information in identifiable form.

Some Components advise that they do provide such information, but some do so upon request.

c. Verification of intent to comply with agency policies and procedures? Yes.

The FISMA question essentially asks whether the Department possesses materials that verify the Department's intent to comply with established Departmental policies. The actions and conduct of the DoD Components and personnel are subject to, and guided by, DoD regulatory authority which sets forth current policies, practices, and procedures. Therefore, Departmental actions and conduct, as well as that of its personnel, are expected to be in accordance, and consistent, with the prescribed norms established by such authority.

IV. **Contact Information**

Title	Name	Phone Number	E-mail
Secretary of Defense	Donald H. Rumsfeld	703-692-7100	
DoD CIO	John G. Grimes	703-695-0348	John.Grimes@osd.mil
DoD IG (Acting)	Thomas F. Gimble	703-604-8300	tgimble@dodig.osd.mil
DoD CISO	Robert A. Lentz	703-695-8705	Robert.Lentz@osd.mil
DoD Senior Privacy Official	Michael B. Donley	703-692-7138	Michael.Donley@osd.mil
Director, DPO	Vahan Moushegian, Jr.	703-607-2943	Vahan.Moushegian@osd.mil
PIA Reviewing Official	Component CIO		

IV. **Safeguarding Personally Identifiable Information**

OMB directed agencies to conduct a review of agency policies and processes, and to take corrective action as necessary, to ensure that the agency has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.

The review was to address all administrative, technical, and physical means used by the agency to control such information, with special emphasis on policies and practices relating to the removal of such information beyond agency premises or control.

And finally, OMB directed that the results of the review should be reported as part of the Annual FISMA Privacy Report.

Upon receipt of M-06-15, the Senior Privacy Official issued implementing guidance to the DoD Components requesting that each conduct such a review and to report the results thereof as part of their Annual FISMA Privacy Report. Subsequently, upon receipt of the OMB FISMA 2006 reporting guidance, the Senior Privacy official issued his implementing guidance for the

ATTACHMENT 2

DoD Privacy Report and provided supplementary guidance as to how they were to report the results of their review. The guidance was as follows:

"Components shall report how the review was conducted, describing in sufficient detail what actions were taken incident to the review, e.g., all component regulatory issuance, policy letters, SOPs, etc. relating to the safeguarding of personally identifiable information were identified and reviewed to ensure that they provide current and updated information, to include whether the prescribed technological controls in place are adequate to meet today's technology threats; spot checks were conducted to verify that established policies and practices are in fact being observed by the Component work force; reporting mechanisms were examined to ensure that they are adequate to accomplish any reporting and/or notification that have to be made when there is a compromise or breach of information; etc.

Because the OMB review requirement was prompted, at least in part, by the theft of a Department of Veterans Affairs laptop computer from the home of one of its employees, the OMB highlighted the fact that the review also should cover agency procedures and restrictions when information is removed from agency premises or control.

Components shall report what their current policies and practices are when information is removed. If there are different policies and procedures for different removal scenarios (e.g., TDY, Telework, working at home, etc.), the different policies should be described, to include what restrictions may apply to removal, whether or not approval must be obtained, what actions are required to be taken if there is a loss or compromise, etc.

If the Components do not have policies or procedures that adequately safeguard personally identifiable information, to include polices on the use of such information off-site, describe what actions are being taken to establish such policies and when it is anticipated that the policies will be established."

Subsequently, OMB issued further guidance as to what actions must be taken to protect personally identifiable information (M-06-16). As briefly discussed in section III.2 above, the DoD CIO has issued implementing guidance designed to ensure that all personally identifiable information not explicitly cleared for public release is protected according to standards prescribed in the DoD CIO issuances. The guidance also directed all information and data owners to conduct risk assessments of compilations of PII and identify those needing more stringent protection for remote access or mobile computing. In support of these requirements, detailed guidance was provided.

The review indicated that the agency overall has adequate safeguards or, where not, actions are being initiated to either enhance the existing safeguards or to establish new safeguards.

The DPO and the Components conducted a review of their Privacy issuances and determined that they were either adequate or were being changed to augment the existing safeguarding requirements. The Components reported on numerous initiatives or actions being taken to strengthen the processes within their Component in this area. In general, all Components focused attention on the adequacy of the safeguards when information is removed from the Component premises or control.

One Component reported that many of its activities had adopted various control measures to provide greater protection to electronic PII records (e.g., use of common identification credentials to access data, policy prohibiting removal of PII from the workplace, etc). Another Component

also implemented new procedures (e.g., stripping Social Security Numbers from records except those required by law or regulation, requiring all PII to be password-protected on all network shared drives, requiring all websites and emails containing or using PII to employ Secure Socket Layer and Public Key Infrastructure, requiring all PII stored on removable storage media or devices be protected by encryption and password protections) or is pursuing new initiatives (e.g., updating current telework policy to include requirements for encryption and and protecting PII and appropriate "data at rest" procedures, promulgating new reporting requirements on PII "spills," etc). Another Component has established a Team to review encryption of sensitive data on mobile computers and devices and to determine under what conditions remote access should be authorized. This Component also is intending to deploy a Host Based Intrusion Prevention System and Network Access Control features to secure remote laptops for telework and travel. Incident to one Component's review, it conducted spot checks of various offices within the Headquarters to determine if individual are aware of, and are in compliance with, established safeguards. Another Component held a two-part Privacy summit for systems managers. At the first summit, the focus was on identifying the systems impacted by the review, and at the second summit, the focus was on whether prescribed safeguards were in place. One agency developed a "Privacy Data Sheet" as a cover to be placed on documents containing privacy-related data. One Component established a Privacy Integrated Project Team, consisting of the Component Privacy Official, the Component CIO, the Director of Human Resources, the General Counsel, and the Director of Enterprise Support, to address multiple privacy related objectives.

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

26 MAY 2006

ADMINISTRATION &
MANAGEMENT

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

SUBJECT: DoD Personnel Responsibility for Safeguarding Personally Identifiable Information

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

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

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

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

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

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

Ralph E Newton

for Michael B. Donley
DoD Senior Privacy Official

Attachment:
As stated

ATTACHMENT 3

FACT SHEET

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

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

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

"DoD Personnel shall:

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

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

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

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

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

DoD FISMA STATUS UPDATE: ENTERPRISE PLAN OF ACTION AND MILESTONES[1]

Significant Deficiency	Description	Status (as of 31 October 2006)	Status (as of 25 April 2007)	Projected Timeline
1. Certification and Accreditation (C&A) Process	Revise DoD security C&A policy and process to improve compliance and provide enterprise management capability	Interim DoD Information Assurance Certification and Accreditation Process (DIACAP) issued 6 July 2006 Pending approval of final DIACAP policy	DIACAP in formal coordination (SD106) with all DoD Components	Expected formal issuance of DIACAP in June 2007
2. Security Controls Not Tested Annually on a Majority of Information Systems		Closed Enterprise-wide, DoD reports 87% security controls tested as of 1 September 2006 66% of DoD Components above 90% as of 1 September 2006	Completed	N/A
3. Contingency Plans Not Tested on a Majority of Information Systems	DoD policy requires testing contingency plans on an annual basis	Closed Enterprise-wide, DoD reports 83.5% contingency plans tested rate as of 1 September 2006 57% of DoD Components above 90% as of 1 September 2006	Completed	N/A

ATTACHMENT 4

[1] This document represents the ASD/NII response to the OMB task requesting information identifying the POA&M status reflected in the agency FY06 Annual FISMA Report

Significant Deficiency	Description	Status (as of 31 October 2006)	Status (as of 25 April 2007)	Projected Timeline
4. Security Plans of Action and Milestones (POA&M) Process	Develop improved and integrated enterprise and Combatant Commands, Services, and Agencies (CC/S/A) process for POA&M reporting and remediation	DoD formal guidance was signed by DoD CIO and issued with annual FISMA Guidance on 4 April 2006 and with Interim DIACAP on 6 July 2006; Action(s) pending OIG concurrence of POA&M process (formalized in DIACAP)	DIACAP, which includes POA&M Process, in formal coordination (SD106) with all DoD Components	Expected formal issuance of DIACAP in June 2007
5. Specialized Information Assurance (IA) Training	Deficiencies identified in: IA Training and Certification; Identification and Tracking Requirement; IA Workforce Management; IA Workforce Reporting and Oversight	DoD 8570.01-M, 19 December 2005, establishes policy, requirements and procedures to resolve these workforce deficiencies These improvements are being tracked and maintained through an IA Workforce Management POA&M	Annual Data call being issued through FISMA reporting process; Components are beginning to populate Defense Civilian Data System (DCPDS) with IA workforce data Defense Integrated Human Resources System (DIMHRS) IA workforce management data requirements are being integrated into second release of DIMHRS Contractor IA workforce data management requirements are being addressed in DoD workgroups	Q1 FY08 integrated with DoD Annual FISMA Report DCPDS updates to be complete Q1 FY08 DIMHRS updates to be completed Q2 FY09 Initial plan for contractor IA workforce data to be developed by DoD by Q4 FY07

Significant Deficiency	Description	Status (as of 31 October 2006)	Status (as of 25 April 2007)	Projected Timeline
6. Information Assurance Awareness and Training	Develop an enterprise-wide strategy to infuse, and continually enhance information assurance awareness and training into programs for all end users; manage and track CC/S/A efforts and ensure integration, coordination, and standardization	DoD 8570.01-M provides specific requirements which have been integrated into the 2006 FISMA reporting guidance	Completed Details addressed in FY06 FISMA Guidance issued March 2006 & Draft FY07 Annual Guidance; DoD policy has been published. Enterprise training is available through Defense Information Systems Agency (DISA); Tracking of IA awareness training is managed through the Annual FISMA reporting process	N/A