Defense Threat Reduction Agency
8725 John J. Kingman Road MSC 6201
Ft Belvoir, VA 22060-6201

AUG 1 9 2008

MEMORANDUM FOR DISTRIBUTION C

SUBJECT: Defense Threat Reduction Agency (DTRA) Directive-Type Memorandum 08-01, Safeguarding Against and Reporting Privacy Breaches

Reference: (a) Office of Management and Budget (OMB) Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" dated May 22, 2007
(b) Office of the Secretary of Defense (OSD) Memorandum (of the same title) dated September 21, 2007
(c) Executive Order 13402, "Strengthening Federal Efforts to Protect Against Identity Theft" May 6, 2006
(d) DoD Interim Guidance dated July 6, 2006, "Certification and Accreditation (C&A) Process Guidance (DIACAP)

Recent government-wide and Department of Defense (DoD) policy require that Federal agencies and DoD components develop and implement procedures to safeguard and prevent the breach of personally identifiable information (PII). Safeguarding PII in their possession is essential to all DTRA personnel: military, civilians, contractors and business partners, to include remote sites, to prevent the compromise or loss of that information.

DoD has integrated new PII requirements into its policy to improve the decision making process relative to breach notification and reporting. See OMB and the OSD memos provided at: http://www.defenselink.mil/privacy/index.html. These new requirements mandate that agencies: review current holdings of PII for purposes of reducing the volume of collected and retained information to the minimum necessary; conduct Privacy Act training for personnel assigned, employed and detailed, to include contractors; report incidents when there is a loss, theft, or compromise of PII; and notify affected individuals when a breach of PII has occurred. These requirements are further outlined in Attachment 1.

This DTRA Memorandum will serve as interim guidance on this subject pending the revision, staffing, and publication of an Instruction. The changes at Attachment 1, "Safeguarding PII and Breach Notification" are effective immediately and will be incorporated into DTRA Privacy Program Instruction 5400.11 within 180 days.

My point of contact for this action is Mr. Andrew Walker, Chief, Mission Support. He may be reached at 703-767-5862.

James A. Tegnelia
Director

Attachment:
As stated

ATTACHMENT 1

Safeguarding PII and Breach Notification

TABLE OF CONTENTS

1. Definitions

2. Training

3. Review of Personally Identifiable Information Holdings

4. Incident Reporting and Handling Requirements

5. Identity Theft Risk Analysis Factors

Enclosure 1
Identity Theft Risk Matrix

Enclosure 2
Certification of Initial/Annual Refresher Training

1. Definitions.

1.1. Personally Identifiable Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. PII may also be used to distinguish or trace an individual's identity, such as their name, date, social security number, and place of birth, mother's maiden name, and biometric records.

1.2. Breach (lost, stolen or compromised information). A loss of control; compromise; unauthorized disclosure, acquisition, or access; or any similar term referring to situations involving an other than authorized purpose where persons other than authorized users have access or potential access to PII, whether physical or electronic.

1.2.1. OMB also stresses that "agencies should bear in mind that notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion." Adverse affect, or risk of harm, is implicitly part of the OMB concept of breach and will be maintained in the DOD definition of breach.

1.2.2. DTRA will utilize the factors as outlined in Paragraph 5 below, "Identity Theft Risk Analysis Factors," to make determinations of risk of harm associated with a breach of PII. These factors are also outlined in the table at Enclosure 1.

1.3. Business Partners. Persons or organizations, to include grantees, federal entities, and companies, seeking to do business with the federal government as a part of the DoD's e-Government initiative.

2. Training.

2.1. Training and communication related to privacy must be job specific and commensurate with an individual's responsibilities. Training is a prerequisite to employee, manager, or contractor permission to access DTRA systems. Finally, such training is now mandatory for all affected DTRA personnel: military, civilians, contractors and business partners, to include remote sites (hereinafter referred to as DTRA personnel).

2.2. To meet these training requirements, all DTRA Associate Directors shall ensure their personnel receive Privacy Act training, as follows:

2.2.1. Orientation Training. Provide all individuals with a basic understanding of the requirements of the Privacy Act and DoD 5400.11-R, Privacy Program Regulation, as it applies to the individual's job performance.

2.2.2. Specialized Training. Apply to the application of specific provisions of the DoD 5400.11-R, Privacy Program, to specialized areas of job performance. Personnel of particular concern include, those who are expected to deal with the news media or public, personnel specialists, special investigators, public affairs officials, Information Technology professionals, and contractors who operate or have access to a system of records.

2.2.3. Management Training. Provide considerations for managers and decision makers to take into account when making management decisions regarding the DTRA PA Program.

2.2.4. Privacy Act (PA) Systems of Records Training. Ensure all individuals, specifically system managers, who work with a PA system of records, are trained on provisions regarding Privacy Act systems of records notices consistent with this instruction.

2.3. Annual refresher training for all DTRA personnel is required to ensure continued understanding of their responsibilities. All DTRA personnel with authorized access to personally identifiable information shall annually sign a certification (enclosure 2) upon completion of: (1) initial training prior to granting access; and (2) annual refresher training. The certification shall also be subject to inspection during reviews by Privacy Officials and/or Inspectors General.

3. Review of Personally Identifiable Information Holdings.

3.1. As required by the Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, DTRA must confirm the establishment, or the process of establishing, PII review plans; and provide a schedule for periodic update reviews of their holdings following an initial review. This review will also serve as a method to reduce the use of PII, specifically the SSN.

3.2. It shall be DTRA policy that the DoD Information Technology Portfolio Repository (DITPR) identify all DTRA automated systems containing PII. DTRA's Privacy Officer and CIO must coordinate to ensure each system is accurate, relevant, timely and complete, except where a Privacy Act exemption rule under 5 U.S.C. 552a(j) & (k) applies. This policy covers both paper and electronic records.

3.2.1. It shall be DTRA policy to conduct periodic updates as required by OMB to:

3.2.1.1. Coordinate reviews of IT systems containing PII on the same annual cycle as required by Policy 4.8 of the Interim Department of Defense (DOD) Certification and Accreditation (C&A) Process Guidance (DIACAP), dated July 6, 2006.

DTRA's Privacy Act Officer will conduct biennial reviews of PA system of records notices.

3.2.2. DTRA's Privacy Act Officer shall report the results of the review of the systems, processes and holdings annually to the Defense Privacy Office (DPO) on the established annual FISMA reporting schedule. The DTRA Privacy Officer will coordinate with the DTRA CIO in submitting quarterly reports to DPO as requested.

4. Incident Reporting and Handling Requirements.

4.1. Agency Reporting Requirements. DTRA SC will report all breaches of PII to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) within 1 hour of becoming aware of the breach. The DTRA Privacy Officer will report all breaches of PII to the DTRA Senior Privacy Official within 24 hours and the DTRA Director and the DPO within 48 hours of becoming aware of the breach.

4.1.1. DTRA shall ensure that their reporting procedures are updated to include notification to banks when the breach involves the loss, theft, or other compromise of government credit cards issued by a bank.

4.1.2. Reporting and Notifications will include breaches involving both electronic and paper documents.

4.2. External Breach Notification Requirements. When making the determination of whether notification of breach is required, the DTRA Director, Enterprise Head, (or geographic director) will assess the likely risk of harm caused by the breached information and then assess the relative likelihood of the risk occurring (risk level).

4.2.1. There are five factors set forth by DoD that will be used to assess the likely risk of harm (see Matrix at Enclosure 1). A wide range of harms will be considered, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach.

4.2.2. DTRA shall be aware that notification when there is little or no risk of harm might create unnecessary concern and confusion. Moreover, documentation of the rationale and the resulting "Risk Level" is required when the risk assessment concludes that notification is not necessary.

4.3. Timeliness of the Notification. Notification to breach victims shall be made your respective office as soon as possible, but no later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained. Notification may be delayed for good cause (e.g., law enforcement authorities request delayed notification). When notification is not made within the 10 day period DTRA

shall inform the Deputy Secretary of Defense why notice was not provided. (OMB guidance states that agencies should provide notification without unreasonable delay, but consistent with the needs of law enforcement and national security.)

4.4. Source of the Notification. Notifications shall be made by the DTRA Director (or the senior-level individual where the loss, theft, or compromise occurred).

4.5. Contents of the Notification. The notification should be in writing and be concise, conspicuous, and in plain language. The notice should include the following elements:

4.5.1. A brief description of what happened, including the date(s) of the breach and of its discovery;

4.5.2. To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, Social Security Number, date of birth, home address, account number, disability code, etc.);

4.5.3. A statement whether the information was encrypted or protected by other means if it is determined that such information would be beneficial and would not compromise the security of the system;

4.5.4. What steps individuals should take to protect themselves from potential harm, if any;

4.5.5. What is being done to investigate the breach, to mitigate losses, and to protect against further breaches, and

4.5.6. Who affected individuals should contact for more information (i.e., designated personnel in the DTRA Enterprise or geographic location where the breach occurred), including a phone number, either direct or toll-free, email address, and postal address. DTRA's Privacy Officer contact information may be included, but only as a secondary point of contact.

4.6. Means of Providing Notification. The preferred method of notification will be made by first-class mail, but other means are acceptable where another means is preferable and contact with affected individuals is reasonably assured.

4.6.1. DTRA policy calls for follow-up written notification after telephonic notification is given. Further, DTRA policy requires that the envelope containing the written notification will be marked "First Class," as provided by the OMB guidance.

4.6.2. A generalized (substitute) notice shall be given to the potentially impacted population by whatever means is most likely to reach them if they cannot readily be identified individually or if they cannot be reached.

4.7. Who Receives Notification. To preserve the public's trust, DTRA policy requires that media notifications be promptly prepared in cases where the breach is significant (i.e., impacting thousands of individuals, or containing highly sensitive PII). Another consideration is that the risks and potential for harm as a result of the breach are greater to the individuals involved than to any investigation resulting from public disclosure of the breach.

4.8. DTRA Public Affairs is responsible for establishing a protocol to determine when a public affairs release on a breach should be made. The DTRA Director, Associate Directors (or geographic director) will make the determination to release the public announcement upon consideration of Public Affair's recommendation.

5. Identity Theft Risk Analysis Factors

5.1. Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals.

5.2. Number of Individuals Affected. The magnitude of the number of affected individuals should not be the only determining factor for whether notification should be provided.

5.3. Likelihood the Information is Accessible and Usable. DTRA shall assess the likelihood PII will be or has been used by unauthorized individuals.

5.4. Likelihood the Breach May Lead to Harm. The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Additional OMB guidance is available at the website provided below:
whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

5.5. Ability of the Agency to Mitigate the Risk of Harm. Within an information system, the risk of harm will depend on how the agency is able to alleviate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of personal information and patterns of suspicious behavior, should be taken.

Identity Theft Risk Matrix

RISK LEVEL DETERMINATION	DATA ELEMENTS	CONSIDERATIONS
High	SSN Name + SSN Name + Medical or Financial	No encryption (FIPS 140-2) or password protection used. Requires notification. Compromise beyond DTRA/DoD control (lost or stolen, possibility PII could be used with malicious intent or to commit ID theft). Compromise within DTRA/DoD with evidence of possible malicious intent.
Moderate	Name + 1 or more personal identifier (not SSN, Medical or Financial)	Password protection used. Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual. Moderate likelihood of harm.
Low	Name only	Encryption (FIPS 140-2) used. Consideration given to unique names; one or only a few in the population or those readily identifiable. No evidence of malicious intent. Low likelihood of harm.

RISK LEVEL DETERMINATION	**DATA ELEMENTS**	**CONSIDERATIONS**
IN GENERAL	All	All actual/suspected PII breaches (paper or electronic) require DTRA SC notification to US-CERT within 1 Hour, to DTRA Privacy Act Officer ASAP, who will notify the Senior Privacy Official within 24 hours, and the DPO and DTRA Director within 48 hours. Affected individuals (based on 5 factor analysis) must be notified within 10 working days. (Number of individuals affected does not determine whether notification is given.) The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. DTRA will thoroughly document the PII breach circumstances and the above decision to notify/not notify individuals. Risk /harm determinations to be made by the DTRA Director /Head of the DTRA Enterprise/geographic director where the PII breach occurred.

Certification of Initial/Annual Refresher Training

"This is to certify that I have received initial/annual refresher training on my privacy and security responsibilities. I understand that I am responsible for safeguarding personally identifiable information that I may have access to incident to performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard personally identifiable information, for improperly using or disclosing such information, and for failure to report any known or suspected loss or the unauthorized disclosure of such information."

(Signature)	(Print Name)
(Date)	(DTRA Office)