U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 13, 2007

**ACTION**

MEMORANDUM FOR: DISTRIBUTION

FROM: Paul A. Schneider
Under Secretary for Management

Hugo Teufel III
Chief Privacy Officer

SUBJECT: Review of Safeguarding Policies and Procedures for Personnel-Related Data

Given the recent data security incident at the Transportation Security Administration, Secretary Chertoff directed the Under Secretary for Management and the Chief Privacy Officer to ensure that appropriate policies and procedures are in place and fully implemented to safeguard personally identifiable information[1] (PII) of our personnel. Personnel-related data is a subset of PII and includes any PII about the Department of Homeland Security (DHS) employees or contractors held in systems such as human capital operations, security operations, financial operations, time and attendance systems, user name and log in systems, travel systems, and any other electronic systems or hard copy records where such information may be found.

Privacy security incidents can occur at any time and any place, wherever appropriate safeguards have not been followed. For this reason, we are directing all Component and Directorates to examine the entire breadth of the organization, even down to the smallest office so that DHS is in a position to better understand and identify possible issues before the next incident occurs.

To accomplish this undertaking, the Under Secretary and the Chief Privacy Officer request each Component and Directorate to do the following:

- **By June 27, 2007**: The Component/Directorate Head shall convene a Component/Directorate-level cross functional review team consisting of representatives from the offices that handle personnel-related data and provide the HQ Privacy Office with the primary point of contact for the team. The Component/Directorate-level review team will conduct a self-assessment of the

---

[1] "Personally identifiable information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual. This definition applies regardless of whether the individual is a U.S. citizen, legal permanent resident, a visitor to the U.S., DHS employee, or contractor.

handling of personnel-related data using the attached self-assessment form. See Attachment 1 for additional guidance.

- **By August 15, 2007**: The Component/Directorate Head shall submit to the Head Quarters (HQ) Privacy Office the completed assessment, along with verification and confirmation as to the accuracy and completeness of the self-assessment. The memo template in Attachment 3 may be used for this purpose. A cross-functional team from the Privacy Office, Human Capital Office, Office of Security, and Office of Chief Information Officer will review the self-assessment for follow-up action as necessary.
- **By September 15, 2007:** The Component/Directorate Head shall certify, using the memo template in Attachment 3, that all employees and contractors with access to personnel-related data have taken mandated privacy and information technology (IT) security awareness training approved or provided by the Chief Information Officer. Component/Directorate Head should submit the certification to the HQ Privacy Office. As part of this training, the Component Head shall emphasize that employees will be held accountable for their actions and subject to appropriate disciplinary action when their conduct fails to conform to Departmental privacy and security policies.
- **By September 15, 2007:** The Component/Directorate Head shall provide copies of the *Protecting & Handling Personnel-Related Data – Quick Reference Guide* in Attachment 2 to all employees as part of the combined training.

The Department takes very seriously its responsibilities to safeguard the personally identifiable information about the people that it employs. With identity theft on the rise creating not only a risk for the individual affected, but also a potential security threat, we must ensure that we do everything possible to safeguard this information. Thus, it is essential to keep the trust of the individuals, whose information we maintain, by protecting it and preventing any unauthorized disclosure. This review and the policies outlined herein intend to help all of us ensure these protections are in place.

*Attachments*

Attachment 1: Review of Personnel-Related Data Policies and Procedures and Self Assessment

Attachment 2: *Protecting & Handling Personnel-Related Data – Quick Reference Guide*

Attachment 3: Verification and Confirmation Memorandum Templates (Self-Assessment and Training Certifications)

*Background Materials*

Attachment 4: DHS Employee Communication, June 8, 2006 from Scott Charbo and Maureen Cooney regarding Data Security and Privacy

Attachment 5: DHS Deputy Secretary Memo, April 26, 2007 regarding Advance Notice to Leadership on Unintentional Release of Privacy Act Protected Information

Attachment 6: Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

Review of PII Policies and Procedures
June 13, 2007

**Distribution List:**

Chief of Staff
Under Secretary, Federal Emergency Management Agency
Under Secretary, National Protection and Programs
Under Secretary, Science and Technology
Under Secretary, Management
General Counsel
Assistant Secretary, Policy
Assistant Secretary, U.S. Immigration and Customs Enforcement
Assistant Secretary/Administrator, Transportation Security Administration
Assistant Secretary, Intelligence and Analysis
Assistant Secretary/Chief Medical Officer, Health Affairs
Assistant Secretary, Legislative Affairs
Assistant Secretary, Public Affairs
Commandant, U.S. Coast Guard
Commissioner, U.S. Customs and Border Protection
Director, U.S. Citizenship and Immigration Services
Director, United States Secret Service
Director, Operations Coordination
Director, Counternarcotics Enforcement
Director, Federal Law Enforcement Training Center
Director, Domestic Nuclear Detection Office
Chief Financial Officer
Inspector General
CIS Ombudsman
Chief Privacy Officer
Officer, Civil Rights and Civil Liberties
Executive Secretariat
Military Advisor

cc: Marta Brito Perez, Chief Human Capital Officer
Scott Charbo, Chief Information Officer
Jerry Williams, Acting Chief Security Officer

Attachment 1

*Review of Personnel-Related Data Policies and Procedures and Self Assessment*

Each Component and Directorate shall identify a cross functional team that is made up of representatives from the offices that handle personnel-related data. Each Component and Directorate must report in writing the name, title, and contact information for the Component and Directorate point of contact directly to Rebecca J. Richards, Director of Privacy Compliance, Privacy Office, by COB June 27, 2007. This Component/Directorate-level team shall identify and review all paper-based and IT related systems that may contain personnel-related data.

The attached self-assessment for the handling of personnel-related data must be verified and confirmed by the Component/Directorate Head and submitted to Rebecca J. Richards, Director of Privacy Compliance, Privacy Office no later than August 15, 2007.

Personnel-related data is a subset of personally identifiable information (PII)[2] and includes any PII about DHS employees or contractors held in systems such as human capital operations, security operations, financial operations, time and attendance systems, user name and log in systems, travel systems, and any other electronic systems or hard copy records where such information may be found.

Personnel-related data can be found throughout a Component/Directorate's operations, not only with those with programmatic responsibility for human capital and security operations, but also those in a management or supervisory role. Information may be both electronic and hard copy, and can be at headquarters, regional, and remote locations.

Privacy security incidents can occur anywhere where appropriate safeguards have not been followed. For this reason we are asking for Components and Directorates to examine the entire breadth of the organization, even down to the smallest office, so that DHS is in a position to understand and identify possible issues before the next incident occurs.

A Departmental cross functional team comprised of representatives from the DHS Privacy Office, Human Capital Office, Office of Security, and Office of the Chief Information Officer will review the self-assessment and may follow up with additional meetings to permit the DHS team to understand Component/Directorates' current handling policies and processes for personnel-related data. This assessment will help ensure that previously issued policy has been implemented fully by the component or will help identify gaps in the implementation. Based on the assessments and follow up meetings, the DHS team will develop Department-wide recommendations.

Attachment 3 provides a template for the verification and confirmation memorandum for the Component/Directorate Head to sign.

---

[2] "Personally identifiable information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, legal permanent resident, or a visitor to the U.S.

Review of PII Policies and Procedures
June 13, 2007

Please provide all written documentation, including the self-assessments and any supporting documentation to Rebecca J. Richards, Director Privacy Compliance, Privacy Office, email: pia@dhs.gov, fax: 703-235-0442. If you have further questions, please contact the Privacy Office at 703-235-0780.

*Attachment 2*

*Training of Employees and Contractors with Access to Personnel-Related Data*

The attached document, *Protecting & Handling Personnel-Related Data – Quick Reference Guide* should be provided to all employees as part of the combined training. This document is also available at www.dhs.gov/privacy under Privacy Reports and Statements.

## Protecting & Handling Personnel-Related Data – Quick Reference Guide

**Do** make sure all personnel-related data is marked "For Official Use Only" or "Privacy Data."

**Do** protect personnel-related data according to the privacy and security safeguarding polices.

**Do** report any unauthorized disclosures of personnel-related data to your supervisor, Program Manager, or Information System Security Manager.

**Do** immediately report any suspected security violation or poor security practices relating to personnel-related data.

**Do** lock up all notes, documents, removable media, laptops, and other material containing personnel-related data when not in use and/or under the control of a person with a need to know.

**Do** log off, turn off, or lock your computer whenever you leave your desk to ensure that no personnel-related data is compromised.

**Do** password protect and as appropriate, encrypt all personnel-related data documents sent via e-mail. Do not include the password in the body of the email containing the attachment.

**Do** destroy all personnel-related data in your possession when no longer needed and continued retention is not required.

**Do** be conscious of your surroundings when discussing personnel-related data. Protect verbal communication with the same heightened awareness as you would paper or electronic personnel-related data.

**Don't** leave personnel-related data unattended. Secure it in a locked drawer, locked file cabinet, or similar locking enclosure, or in a room or area where access is controlled and limited to persons with a need to know.

**Don't** take personnel-related data home, in either paper or electronic format, without written permission of your supervisors, office chief, or Information Security Systems Manager, as required.

**Don't** discuss or entrust personnel-related data to individuals who do not have a need to know.

**Don't** discuss personnel-related data on wireless or cordless phones unless absolutely necessary. Unlike landline phones, these phones can be more easily intercepted.

**Don't** put personnel-related data in the body of an e-mail. It must be password-protected as an attachment.

**Don't** dispose of personnel related data in recycling bins or regular trash unless it has first been shredded.

*Attachment 3*

*Verification and Confirmation Template*

August 15, 2007

MEMORANDUM FOR: Paul A. Schneider
Under Secretary for Management

Hugo Teufel, III
Chief Privacy Officer

FROM: <<COMPONENT HEAD/DIRECTORATE HEAD>>

SUBJECT: Verification and Confirmation of the Self-Assessment regarding Safeguarding Policies and Procedures for Personnel-Related Data at <<COMPONENT/DIRECTORATE >>

This memorandum verifies and confirms that <<COMPONENT/DIRECTORATE>> has completed the attached self-assessment and it is accurate and complete as of August 15, 2007.

_____

Head of Component/Directorate Signature/Date

*Training Certification Template*

September 15, 2007

MEMORANDUM FOR: Paul A. Schneider
Under Secretary for Management

Hugo Teufel, III
Chief Privacy Officer

FROM: <<COMPONENT HEAD/DIRECTORATE HEAD>>

SUBJECT: Certification of Privacy and Security Training at <<COMPONENT/DIRECTORATE>>

This memorandum certifies that all employees of <<COMPONENT/DIRECTORATE>> have completed the combined Privacy and Information Security Awareness Training.

_____

Head of Component/Directorate Signature/Date