From: DHS Employee Communications
Sent: Thursday, June 08, 2006 4:16 PM
To: ^DHS-ALL
Subject: Data Security and Privacy

MEMORANDUM FOR: DHS EMPLOYEES AND CONTRACTORS

FROM: Scott Charbo /s/
Chief Information Officer

Maureen Cooney /s/
Acting Chief Privacy Officer

SUBJECT: Data Security and Privacy

Recent news reports of the theft of personally identifiable information of more than 26 million Veterans provides a critical reminder of the care with which Department of Homeland Security employees and contractors must treat this type of sensitive information. The best of intentions to protect sensitive data are no substitute for strong privacy and security controls, as data breaches, both intentional and inadvertent, have become more common. At DHS, we need to continue to take prudent steps to handle and safeguard personally identifiable information.

DHS Management Directive 0470.2, Privacy Act Compliance, specifies the responsibilities of all DHS personnel to treat personally identifiable information respectfully and in compliance with the requirements of the Privacy Act and other applicable statutory privacy requirements. The Privacy Act requires that agencies maintain only such information about individuals that is relevant and necessary to accomplish its purpose. The Privacy Act also requires that the information be maintained in systems -- electronic and paper -- that have the appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against threats or hazards to the information's security.

DHS employees should take the following steps to help ensure compliance with these requirements:

- Share or discuss sensitive personal information **only** with those personnel who have a **need to know** it for purposes of their work.
- Promptly report all suspected compromises of sensitive information, especially information containing personal privacy data. Components are reminded to ensure that all assigned personnel are familiar with the reporting procedures.
- Do not leave work folders containing sensitive personal information unattended; this information should be maintained either in secured file cabinets or on computers that have been secured. Passwords should be used when sharing sensitive personal information.
- Do not remove records about individuals from DHS, unless you obtain clearance from a supervisor and sufficient justification, as well as evidence of information security, has been presented.
- Dispose of personal information appropriately -- use burn bags for hard copy records, erase electronic records.

- Keep the use of social security numbers to a minimum. The SSN was never intended to be an all-purpose personal identifier, and to thwart identity thieves it is important that these numbers are used sparingly and judiciously.

In addition to employees taking these practical steps for protecting privacy related information, the Department's Chief Information Security Office continues to enforce policies and procedures for protecting personally identifiable information online. But, these collective efforts are only as good as your own, so we ask for your continued efforts to safeguard the personally identifiable information with which DHS has been entrusted.

If you have questions, further information is available from DHS component Information Systems Security Managers and Privacy Officers or by calling the DHS Privacy Office at 571-227-3813.