WRITTEN TESTIMONY

of

MARY ELLEN CALLAHAN

CHIEF PRIVACY OFFICER

DEPARTMENT OF HOMELAND SECURITY

Before the

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT

Release Date: July 31, 2012

Good morning, Chairman Akaka, Ranking Member Johnson, and Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss my role as the Department of Homeland Security's (DHS) Chief Privacy Officer, the Privacy Act, and the collaborative achievements of the Privacy Committee of the Federal Chief Information Officers Council.

Role of the DHS Chief Privacy Officer

As you know, the Department of Homeland Security (DHS) is the first department in the federal government to have a statutorily mandated privacy officer. I have had the pleasure of serving in this role since March 2009. The Homeland Security Act grants the Chief Privacy Officer primary responsibility for ensuring that privacy considerations and protections are comprehensively

integrated into all DHS programs, policies, and procedures.[1] Pursuant to my statutory authority, I am tasked with assuring that the Department's use of technologies sustains and does not erode privacy protections relating to the use, collection, and disclosure of personal information. I also ensure that personal information contained in Privacy Act systems of record is handled in full compliance with fair information practices, as set forth in the Privacy Act of 1974, as amended.[2] To achieve this mandate, I lead a dedicated staff of privacy professionals who comprise the DHS Privacy Office.

The mission of the DHS Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. My staff work to achieve its mission by fostering a culture of privacy and transparency; demonstrating leadership through policy and partnerships; providing outreach, education, training, and reports; conducting robust oversight; and ensuring that DHS complies with federal privacy, confidentiality, and disclosure laws, policies, and principles.

It is my pleasure to share with you today a few examples of the DHS Privacy Office's many recent achievements in privacy protection. Last year, we issued Department Directive 047-01, which formalizes the privacy-related responsibilities of DHS personnel and the processes in place to ensure compliance with applicable laws and policies. Two weeks ago, we hosted a successful public meeting of the DHS Data Privacy and Integrity Advisory Committee, which provides advice on privacy-related matters to the Chief Privacy Officer and the Secretary of Homeland Security. In addition, we engage in ongoing collaboration with the DHS Office for

[1] 6 U.S.C. § 142.
[2] 5 U.S.C. § 552a.

Civil Rights and Civil Liberties to provide comprehensive, on-site training to fusion centers from Alaska to Tennessee.

Many of my authorities are similar to those of other federal Chief Privacy Officers. I am unique, however, in that my statutory mandate also includes the authority to investigate Department programs and operations; to issue subpoenas to non-federal entities; and to administer oaths, affirmations, and affidavits necessary to conduct investigations. During my tenure, I have led three investigations of significant non-compliance with Departmental privacy policy. One investigation concerned a privacy incident involving loss of an unencrypted flash drive with financial audit data that contained Sensitive PII. In February 2011, I published a report detailing my findings and setting forth proactive recommendations to prevent and mitigate similar privacy incidents.[3]

The second investigation involved a Component's use of social media for operational purposes without appropriate oversight or privacy protections. After determining that the Component's use of social media was not in compliance with Department privacy policy, my Office provided the Component a set of recommendations that we then used to develop a Department-wide Directive on privacy and social media and the Component has since been in compliance.[4] Additionally, the Directive and its associated Instruction detail specific steps Components must take before engaging in the operational use of social media, including documenting their authority, providing annual training to authorized employees, and creating specific authority-based Rules of

[3] U.S. Department of Homeland Security, Privacy Office, *OIG Privacy Incident Report and Assessment* (February 2011), http://www.dhs.gov/xlibrary/assets/privacy/priv-oig-privacy-incident-report-assessment-022011.pdf.
[4] U.S. Department of Homeland Security, *Privacy Policy for Operational Use of Social Media, Directive 110-01* (June 8, 2012), http://www.dhs.gov/xlibrary/assets/foia/110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf.

Behavior. This investigation improved awareness of privacy concerns and resulted in my Office providing improved standards for operational use of social media to the entire Department.

My third and most recent investigation was prompted by a referral from the DHS Office of the Inspector General. Following the referral, I initiated the investigation in order to determine whether a DHS Component's information sharing pilot with an external agency complied with DHS privacy policy and the Privacy Act and my office recently concluded this investigation.

My office remains vigilant and I use my investigatory authority judiciously and thoughtfully. We consider investigations when my privacy authority is impacted, or when the Department as a whole can establish best practices, as occurred with social media. We thoroughly examine potential violations of Department privacy policy and will not hesitate to invoke my investigative authority where warranted.

Consistent with the Office's unique position as both an advisor and an oversight body for the Department's privacy-sensitive programs and systems, I recently approved the creation of a new Privacy Oversight group within the DHS Privacy Office. This group is dedicated to monitoring, investigating, and otherwise conducting robust oversight of DHS activities to ensure compliance with Department privacy policy. In addition to conducting investigations of privacy non-compliance, the Oversight team has instituted a series of Privacy Compliance Reviews to improve a program's ability to comply with assurances made in Privacy Impact Assessments, System of Records Notices, and formal information sharing agreements. Privacy Compliance

Reviews may result in recommendations to a program, updates to privacy documentation, informal discussions on lessons learned, or a formal internal or publicly available report.

One specific example of my office's privacy efforts that you requested I discuss today is our response to the Office of Management and Budget's (OMB) guidance on safeguarding personally identifiable information (PII). OMB Memorandum M-07-16 required agencies to develop and implement a policy on breach notifications, which DHS refers to as privacy incidents.[5] In September 2007, in response to the OMB memo, the DHS Privacy Office distributed its *Privacy Incident Handling Guidance* throughout the Department to inform employees of their responsibilities to safeguard PII, regardless of format.[6] In addition, the *Privacy Incident Handling Guidance* provided detailed information on how to handle all stages of privacy incidents, including reporting, escalation, investigation, mitigation, notification, and closure.

The Department continues to actively implement OMB Memorandum M-07-16. Earlier this year, my Office revised its *Privacy Incident Handling Guidance* to better reflect privacy incident handling procedures based on observed best practices.[7] We also issued a *Handbook for Safeguarding Sensitive Personally Identifiable Information*, which establishes minimum standards for how Department personnel should protect Sensitive PII.[8] To ensure that staff are

[5] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).
[6] Information may exist in paper, electronic, web-based, or other formats, for example.
[7] U.S. Department of Homeland Security, *Privacy Incident Handling Guidance* (Revised January 26, 2012), http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.
[8] U.S. Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information* (March 2012), http://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf.

cognizant of PII protections, we also updated our annual online training, which is mandatory for all DHS employees and contractors.

The Privacy Act of 1974

The Privacy Act was passed in an era before electronic communications and databases were the norm at federal agencies. As such, the Act did not fully contemplate that multiple entities within the Executive Branch may use the same types of records or operate similar systems. Nonetheless, many of the concepts embedded in the original Act are flexible enough to permit similar records to be treated consistently, regardless of whether they are located at one agency or another. One example of this is the government-wide Systems of Records Notices (SORN), which was developed by the Office of Personnel Management to cover all personnel records across the Executive Branch and ensure that they are treated consistently. DHS employs a similar practice of treating like records consistently under the Privacy Act. For security personnel records, for example, DHS has a single SORN to ensure consistent treatment, regardless of which component maintains the record. DHS also has a single SORN for all Department contact lists regardless of the list's location or format. The practices described above promote efficiency and Privacy Act compliance, while ensuring that the public understands how information is used and stored.

Privacy Committee of the Federal Chief Information Officers Council

One method to address modern challenges of implementing the Privacy Act is to share best practices among federal privacy officials. Formal Council-level bodies exist for many federal chief officers, including the Chief Financial Officers, Chief Information Officers, and Chief Human Capital Officers. Though no formal Council-level body exists for Chief Privacy Officers,

I am proud to serve as Co-chair of the Privacy Committee of the Federal Chief Information Officers Council.

The Privacy Committee was initially formed in response to the need to coordinate on shared challenges, such as information sharing and protection of personally identifiable information. Since its formal establishment in 2009, the Committee has successfully functioned as a consensus-based forum for the development of privacy policy and protections throughout the federal government. The Committee currently serves as the interagency coordination group for federal Chief Privacy Officers and Senior Agency Officials for Privacy. It provides an important venue in which to share experiences, training, innovative approaches, best practices, and safeguards with other federal privacy professionals.

One example of how the Committee has benefited the federal privacy community at large is through its interagency training sessions. In the first year of the Administration, the Committee hosted a privacy training "boot camp" for new senior privacy officials to enhance their ability to promote privacy protection in their respective agencies. The Committee has shared additional knowledge and first-hand experience with the privacy community, including public stakeholders, through three plenary Summits and focused events on international privacy and other timely topics.

In addition to hosting government-wide training, the Committee has led development of privacy standards and safeguards for emerging technologies, such as cloud computing and social media. The Committee seeks opportunities to promote privacy through partnership with other federal

entities, such as the National Institute of Standards and Technology (NIST). The latest draft of NIST's security guidance, which applies to information systems across the federal government, reflects the joint development of comprehensive privacy controls informed by the Committee's extensive privacy expertise.[9] The achievements of the Privacy Committee indicate the vital role it serves in promoting consistent federal privacy policy, and it has been an honor to serve as one of the Committee's chairs.

Conclusion

The efforts of the Privacy Committee and of the DHS Privacy Office benefit greatly from the support of this subcommittee and its members. Going forward, I am confident that the Department will continue to embed privacy and confidentiality protections throughout its programs and systems. I am happy to answer any questions you may have.

#####

*[9] U.S. Department of Commerce, National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, Initial Public Draft (February 2012), http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf.