**WRITTEN TESTIMONY**

***of***

**KAREN NEUMAN**

**CHIEF PRIVACY OFFICER**

**DEPARTMENT OF HOMELAND SECURITY**

***Before the***

**UNITED STATES SENATE**

**COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**

**SUBCOMMITTEE ON THE EFFICIENCY AND EFFECTIVENESS OF**

**FEDERAL PROGRAMS AND THE FEDERAL WORKFORCE**

**November 19, 2013**

Good morning Chairman Tester, Ranking Member Portman, and Members of the Committee. I appreciate the opportunity to appear before you today to discuss the role of the Department of Homeland Security (DHS) Privacy Office and how our oversight responsibilities complement our policy and compliance functions to ensure privacy rights are protected as the Department carries out its various, critical missions.

As you know, Section 222 of the Homeland Security Act of 2002 established the Chief Privacy Officer as the first statutorily mandated privacy official in the federal government. Under the Homeland Security Act, the Privacy Office is charged with ensuring the Department's use of technology sustains and does not erode privacy protections relating to the use, collection, and disclosure of personally identifiable information (PII). In this effort I am assisted by highly qualified privacy professionals who also work to ensure that DHS's collection and use of information is in full compliance with fair information practice principles (FIPPs).

It is important to note that the Privacy Office is not a pure oversight office. We manage a portfolio of statutory responsibilities that includes oversight in addition to policy and compliance functions. Our challenge, therefore, is to understand how oversight responsibilities impact our compliance and policy functions, and blend them into a coordinated mission set that the Privacy Office can implement in support of privacy interests for activities across the Department.

**The Privacy Office is a Policy Office**

Section 222 of the Homeland Security Act established the Chief Privacy Officer as the principal policy advisor to the Secretary of Homeland Security for privacy matters. This highly specialized

role is a separate and distinct role from the Department's other policy-making functions. In this capacity, the Privacy Office has issued a number of Department-wide policies including the DHS-wide Management Directive on Privacy Policy and Compliance as well as policies on the use of social security numbers and social media at DHS, loss or unauthorized use or disclosure of PII, and protection of terrorism-related information shared within the Information Sharing Environment.

In addition to crafting privacy policy guidance, the Privacy Office focuses on operationalizing privacy at DHS by building a first-rate privacy compliance team and process designed to ensure that program managers and frontline personnel understand how their use of data impacts privacy and that systems are designed and operate in full compliance with all applicable laws. We work closely with components and offices—at each stage of program or system development—to "bake privacy in" by implementing the FIPPs as set forth in DHS Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security. The Privacy Impact Assessment (PIA) has also become a powerful tool for accomplishing this mandate.

*The PIA as a Document and a Process*

A PIA is a document that serves a very important function by providing transparency into DHS operations and describing the ways in which privacy has been built into DHS information technology systems, programs, initiatives, and rulemakings. DHS has published more than 500 PIAs on its website where interested citizens and organizations can learn about how information is collected, used, and shared by the Department.

The PIA is also a process. To conduct a PIA, the Privacy Office partners with mission personnel across the Department, component privacy staff, and other stakeholders including the Office of the General Counsel (OGC), the Office for Civil Rights and Civil Liberties (CRCL), the Office of Policy, and others. Under the direction of the Privacy Office, key organizations work together at the earliest stages of system development to identify potential privacy risks and to mitigate them, before they harm individual privacy. The evaluation and mitigation process is repeated and refined at each stage of development, as uses of information and technological capabilities evolve.

The result of this process is the written PIA document, which reflects our involvement even in the early development of the Department's sensitive programs, systems, or other initiatives. Indeed, we believe that—for the majority of our work—privacy is best protected when we provide advice on privacy requirements and policy at every stage in a program or system's life cycle.

**The Privacy Office is an Oversight Office**

In addition to its role as a policy office, the Privacy Office serves an important oversight role at DHS as part of a layered approach to oversight that includes the component privacy officers at DHS and the DHS OIG, GAO, Congress, the Office of Management and Budget (OMB), and the Privacy and Civil Liberties Oversight Board (PCLOB), and the American public, who are an important part of the Nation's privacy dialogue and informed, in part, through our published PIAs and other efforts to enhance transparency.

In 2007, Congress amended Section 222 of the Homeland Security Act to include additional oversight authorities, including: the power to investigate Department programs and operations; to issue subpoenas to non-federal entities; and to administer oaths, affirmations, and affidavits necessary to conduct investigations. In 2012, the Privacy Office fully implemented these changes by creating the Privacy Oversight Team, responsible for Privacy Compliance Reviews (PCRs), privacy investigations, privacy incident response, and privacy complaint handling and redress. To accomplish their mission, the Oversight Team has forged close working relationships with other oversight offices like the OIG and redress offices like DHS Travelers Redress Inquiry Program (TRIP).

In the past 12 months, the Privacy Oversight Team conducted six PCRs, which are a hybrid of investigative activities and collaborative decision-making. They are designed to improve programs' ability to comply with the assurances to protect privacy reflected in PIAs, Privacy Act System of Record Notices, which are published in the Federal Register, and Information Sharing Access Agreements, which establish terms and conditions—including privacy protections—for receiving PII from DHS. The Privacy Office collaboratively undertakes PCRs of high-profile privacy-sensitive programs and partners with programs to identify and rectify any compliance gaps and design mutually-acceptable paths to improvement. Examples of programs examined include the Department's use of social media for situational awareness, DHS's participation in the Nationwide Suspicious Activity Reporting Initiative, and the Department's implementation of the 2011 U.S.-EU Passenger Name Record (PNR) Agreement. These and other PCRs may

result in recommendations for additional privacy protections, updates to existing privacy compliance documentation, and presentations of lessons learned.

When necessary, and as authorized by Congress, the Privacy Office has conducted a number of investigations in the event of significant non-compliance with Departmental privacy policy. For example, one investigation concerned a privacy incident involving loss of an unencrypted flash drive with financial audit data that contained Sensitive PII. In February 2011, the Privacy Office published a report with detailed findings, setting forth proactive recommendations to prevent and mitigate similar privacy incidents.

The Privacy Office also conducts a number of rolling oversight reviews. These include:

- Intelligence Products Review – The Privacy Office provides same-day review of finished intelligence products disseminated to fusion centers and threat briefings given to the private sector.
- Automated Targeting Rules Review – The Privacy Office, along with CRCL and OGC, conduct quarterly reviews of scenario-based counterterrorism automated targeting rules that DHS uses to prioritize passenger screening efforts at airports and at the U.S. border.
- Quarterly Metrics Reporting Review – As part of the information sharing agreements between DHS and the National Counterterrorism Center (NCTC), the two organizations hold quarterly meetings as required by the agreements. Once again, the Privacy Office teams with CRCL, OGC, and representatives from the Office of Intelligence and Analysis and component data stewards to review reporting metrics stemming from NCTC's access to and use of DHS data.

**Privacy Office Oversight Part of a Layered Approach to Oversight**

The DHS Privacy Office is able to manage the dual role of being both policy advisor and oversight office because of our collaboration with the DHS OIG and GAO. Both offices have built exceptional audit teams to examine privacy issues and the DHS Privacy Office is a frequent participant in these audits, which reinforce our efforts to protect privacy and as a driver of best-practices when our own actions are reviewed.

Component Privacy Officers at DHS serve a vital role within their component's programs and initiatives, greatly enhancing the effort to bake privacy in across the Department. These officials, implementing policy developed by the Privacy Office and ensuring compliance, serve as a key driver in helping systems, programs, initiatives, and rulemakings address privacy as part of their development. These Component Privacy Officers also enhance the oversight activities by participating in PCRs, privacy investigations, and incident responses. They are an important source of recommending programs that the DHS Privacy Office may wish to review.

In addition, OMB provides oversight on privacy issues. For example, OMB reviews our Federal Information Security Management Act (FISMA) privacy scores that we submit annually, along with reports on our activities required every quarter under Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*.

We are also pleased with the reconstitution of the Privacy and Civil Liberties Oversight Board (PCLOB), which is charged with, among other things, analyzing and reviewing actions the

executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties. We interact and consult regularly with the PCLOB as part of these efforts.

Through these efforts and others we hope to provide the public with a greater understanding of privacy risks and the steps we take at DHS to mitigate those risks.

**Conclusion**

Thank you for the opportunity to discuss the DHS Privacy Office and our privacy oversight role. Our unique challenge is to ensure our oversight activities work in harmony with our compliance and policy functions. This effort is supported by the existence of and partnership with the Department's component privacy officers, oversight offices like the DHS OIG and GAO, as well as our relationship with Congress, OMB, and the PCLOB. I look forward to answering your questions.