WRITTEN STATEMENT

OF

HUGO TEUFEL III
CHIEF PRIVACY OFFICER
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

FOR A HEARING ENTITLED,

"PROTECTING PERSONAL INFORMATION: IS THE FEDERAL GOVERNMENT DOING ENOUGH?"

JUNE 18, 2008

Introduction

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is an honor to testify before you today on the progress of the Privacy Office at the Department of Homeland Security (DHS) and to review the findings and recommendations of the recent report on the framework of Federal privacy law by the Government Accountability Office (GAO). I am particularly pleased to testify again with Linda Koontz, who has become quite familiar with the DHS Privacy Office and our efforts to protect privacy within Departmental Programs. I take great pride in the fact that in many cases her team has found elements of our work to praise, particularly the increasing number and quality of our Privacy Impact Assessments (PIA), the bedrock of a meaningful privacy compliance program. In the rare instances where she and her team found us wanting, I believe their sound recommendations were extremely useful in support of our never-ending mission to improve.

Because this is my first time appearing before this Committee, and indeed any committee of the Senate, I would like to introduce myself and my office. I was appointed Chief Privacy Officer of the U.S. Department of Homeland Security by Secretary Michael Chertoff on July 23, 2006. In this capacity and pursuant to Section 222 of the *Homeland Security Act of 2002*, 6 U.S.C. § 142, my office has primary responsibility for privacy policy at the Department, to include: assuring that the technologies used by the Department to protect the United States sustain, and do not erode, privacy protections

relating to the use, collection, maintenance, and disclosure of personal information; assuring that the Department complies with fair information practices as set out in the *Privacy Act of 1974*; conducting PIAs of proposed rules at the Department; evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government; coordinating with the Officer for Civil Rights and Civil Liberties to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and preparing an annual report to Congress on the activities of the Department that affect privacy. To these duties, the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53) added the specific responsibility to conduct privacy impact assessments which was originally required by the E-Government Act of 2002, as well as to provide privacy training to a number of specific programs, coordinate efforts with the Office of Inspector General to investigate privacy complaints, and to issue additional reports to Congress relating to our efforts generally and to the Department's data mining programs. Additionally, I am responsible for overseeing DHS' implementation of privacy-related regulations and policies.

Finally, I also serve as the Department's Chief Freedom of Information Act (FOIA) Officer. In this role, I assure consistent and appropriate Department-wide statutory compliance and harmonized program and policy implementation.

The GAO Audit

Earlier this year, GAO conducted a review of the legislative framework for protecting Personally Identifiable Information (PII) and will be issuing a report entitled, "PRIVACY: Alternatives Exist for Enhancing Protection of Personally Identifiable

Information." My office supported this engagement, participating in interviews with members of Linda Koontz's team and providing insights into our own privacy compliance methods. In its report, GAO recommended that Congress consider amending both the Privacy Act and *E-Government Act of 2002* in order to "revis[e] the scope of laws to cover all PII collected, used, and maintained by the Federal Government; set[] requirements to ensure that the collection and use of PII is limited to a stated purpose; and establish[] additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices."

Because there were no recommendations directed to DHS or the DHS Privacy Office, in particular, my office did not submit any formal response. Informally, however, we objected to GAO's use of the word "adequacy" to frame its review, for this reason: Adequacy is a term-of-art used by the European Data Protection Authority. Countries outside of Europe deemed to have "adequate" local data protection regimes operate under one set of rules covering international data flows, all others must follow an increased administrative burden. Europe has never found the U.S. adequate creating complications in our commercial and government-to-government relationship with Europe for many years. While it is both helpful and proper for GAO to review the sufficiency of the U.S. data protection framework—or any other synonym for adequacy—it is decidedly unhelpful for them to use language that may be misunderstood by U.S. allies and further hamper vital relationships.

Privacy Compliance - DHS use of the Fair Information Practice Principles

Of course, I share GAO's goal of enhancing privacy protections surrounding the use of the PII government-wide. At DHS, the Privacy Office helps programs achieve this

by maintaining a robust Privacy compliance program. The Privacy Act articulates concepts of how the Federal Government should treat individuals and their information, and imposes duties upon Federal Agencies regarding the collection, use, dissemination, and maintenance of PII. The Homeland Security Act, Section 222(a)(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. These principles first appeared in the HEW Report, which was the basis for the passage of the Privacy Act. The FIPPs account for the nature and purpose of the information being collected, maintained, used, and disseminated in relation to DHS' mission to preserve, protect, and secure. They are: Transparency; Individual Participation; Purpose Specification; Data Minimization; Use Limitation; Data Quality and Integrity; Security; and Accountability and Auditing.

Two of GAO's three matters for Congressional consideration are intended to bolster at least four of the FIPPs. For instance, setting requirements to ensure that the collection and use of PII is limited to a stated purpose may enhance the Principles of Purpose Specification, Data Minimization, and Use Limitation. In addition, establishing additional mechanisms for informing the public about privacy protections are intended to enhance the Transparency and Individual Participation Principles.

In general, I have found that strong implementation of the Transparency Principle tends to enhance implementation of the rest of the FIPPs. PIAs and System of Record

Notices (SORNs) are DHS's principal methods of informing the public about the collection, use, maintenance and dissemination of PII. For this reason, the Privacy Office regularly reviews and improves our PIA and SORN guidance, a commitment noted approvingly by GAO. Our Director of Compliance, Rebecca Richards, makes sure these improvements are widely disseminated and understood by her colleagues in the Department, and indeed, the rest of the Federal Government. On May 28, 2008, Ms. Richards delivered her latest PIA and SORN Workshop to more than 125 interested participants from across the government.

In addition to updating and disseminating our guidance, the Privacy Office also updates the PIAs it has already issued. As programs change over time and decisions are made that impact privacy interests, the Privacy Office reexamines the use of PII and issues a new PIA, enhancing understanding of the current state of the program.

Of course, Transparency is furthered through the Privacy Office's practice of publishing our Department's SORNs and as many of the Department's PIAs as is consistent with National Security on our public website, www.dhs.gov/privacy. I note that the Privacy Office conducts PIAs on even the most highly classified programs of the Department. I and a number of my staff carry sufficient security clearances in order to gain full access to the details of such classified programs. Although the PIAs for these may not be made public for many years, in my opinion they still promote the FIPPs because various oversight organizations—GAO, Congress, and the DHS Office of Inspector General, for instance—can use the document to understand the program and its privacy protections. More importantly, such classified or CUI documents are useful to the program to catalogue and understand their own uses of information, including PII.

Implementing OMB and other Guidance

The DHS Privacy Office also fulfils its privacy responsibilities by faithfully executing OMB and other Administration guidance. *The President's Identity Theft Task Force Report* (I.D. Task Force Report), for instance, recommended that Federal Government reduce the unnecessary use of Social Security Numbers (SSN), recognizing that valid SSNs are valuable pieces of information for identity thieves. Less than two months after this report was published, the Privacy Office issued a memo entitled *Use of Social Security Numbers at the Department of Homeland Security,* DHS Privacy Policy Memorandum 2007-02. This policy sets forth the requirements for existing and new programs wishing to continue or initiate use of SSNs, and limits those uses to those that are required by law or pursuant to a specific authorized purpose. Where such use is permitted, the policy also sets limits and/or standards relating to notice to the public, collection and use, security of systems containing SSNs, and retention. We have already begun the process of cataloging and reducing the use of SSN at the Department, and we anticipate this process will lessen the likelihood that PII collected, used, or held by the Department will ever contribute to identity theft.

The Privacy Office has also implemented OMB guidance that followed on the heels of the I.D. Task Force Report. On May 22, 2007, OMB issued a Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. This guidance required Federal agencies to develop a breach notification policy while ensuring proper safeguards are in place to protect PII. In September 2007, then, the Department issued its *Privacy Incident Handling Guidance* (PIHG), which

frames the response mechanisms DHS employs to reduce the risk of identity theft following a loss of or unauthorized access to PII.

These are just two examples of the role OMB and the Administration play in establishing privacy policy. There are numerous other examples.

Congress Should Consider the Consequences of any Changes to Federal Privacy Law

During my review of GAO's draft report, I had an opportunity to review also OMB's written response to GAO, which I understand will appear in whole as an attachment to the final report.

Let me echo two themes in OMB's response to the then-draft report. First, OMB and I agree that Congress should consider any changes to Federal privacy law—in particular the Privacy Act and E-Government Act—in the broader context of privacy laws enacted by Congress. To the examples cited by OMB, I would add the Homeland Security Act. The Homeland Security Act, amendments to it, and subsequent legislation integrated privacy into the Department in a way targeted at its unique mission. As OMB noted in its letter, Congress has accomplished this integration at other agencies.

Related to looking at each individual agency and policy area, I would like to note that, regardless of how long the list of requirements is, leadership, good judgment, and the collaboration of program owners is essential for strong privacy at any agency. For example, more than 20 percent of DHS' PIAs were not strictly required by E-Government, and that number has trended higher in recent years. The E-Government Act provided a strong 80 percent baseline, but the 20 percent was a result of keen leadership attention to privacy in every facet of the Department's operations. In the end, it may be the last 20 percent will always be identified and addressed through direct, hands on, work

with the operational components and cannot be written ahead of time through legislative requirements.

Second, I join OMB's request that Congress fully examine potential implications of any change to Federal privacy law. Since there is no specific language to comment on within the GAO draft report, I will point to a relatively minor matter we are dealing with within the DHS Privacy Office following enactment of the 9/11 Commission Act, passed during the last session of Congress. We are, of course, busy implementing the many sections related to the Privacy Office. However, Section 803 requires that Privacy Officers "consider whether… the need [for a particular] power is balanced with the need to protect privacy[.]" This new language endorses a "balance" paradigm that we in the Department have explicitly rejected.[1] Respecting privacy is one of the Department's primary missions, and crafting well considered PIAs and SORNs as part of a robust privacy compliance program will enhance program performance, even in fulfilling its homeland security missions. This is an important message the Privacy Office uses to integrate privacy into programs in the earliest stages of development, or as we sometimes say, to bake privacy in. As programs work with the Privacy Office to complete these documents, they must carefully examine their proposed use of PII, within the context of the FIPPs, including critical threshold questions like "What is our authority to collect this information?"; "What are we going to do with this information."; and "What information do we actually NEED?" We have found that this examination imposes an important discipline on programs that ultimately serves their homeland security missions well.

[1] See, e.g., DHS Leadership Journal: A Question of Balance, Teufel III, Hugo, November 23, 2007 (available online at http://www.dhs.gov/journal/leadership/2007/11/question-of-balance.html); DHS Leadership Journal: Privacy *And* Security, Chertoff, Michael, September 26, 2007 (available online at http://www.dhs.gov/journal/leadership/2007/09/privacy-and-security.html).

In all candor, we are still learning how the new language in Section 803 of the 9/11 Commission Act impacts our efforts to work with programs to improve their performance from the beginning, while at the same time being required to evaluate how the need to preserve privacy must limit their proposed objectives—a perspective we do not adhere to.

I am not here to ask for a reconsideration of this portion of the 9/11 Commission Act. I raise it only because this well-intentioned language may have consequences that were not foreseen, and which may ultimately hamper our efforts. It is not hard to imagine that efforts to amend the Privacy Act or E-Government Act will have far greater impact than the example I cite. I can only urge this Committee to make sure those potential implications are deliberately considered and well understood before they are enacted. Once enacted, laws are difficult to amend. As Congress considers amending the government-wide privacy statutory framework, I ask that Congress also recognize: 1) the value of its oversight as a tool to strengthen protections on personally identifiable information, and 2) the value of privacy legislation precisely targeted at specific issues. The DHS Privacy Office stands ready to work with Congress and the President to evaluate any proposed changes.

Conclusion

In the past five years, the DHS Privacy Office has built what I believe is a model privacy compliance program, implementing not only the Privacy Act and E-Government Act, but utilizing our inherent authority to examine the privacy impact of programs, offices, rules, and activities under Section 222 of the Homeland Security Act. Congress, too, has endorsed an increased use of the PIA in particular, by requiring PIAs for specific

programs. These developments did not require amendment of either the Privacy Act or the E-Government Act. Yet if Congress should consider amending these authorities, it should be done with full cognizance of the potentially far-reaching consequences.

I thank the Committee and welcome your questions.