WRITTEN STATEMENT

OF

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

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

SEPTEMBER 6, 2007

Introduction

Chairman Thompson, Ranking Member King, and Members of the Committee, I thank you for the opportunity to discuss the Privacy Office's efforts to protect privacy within the National Applications Office (NAO) of the Department of Homeland Security (DHS).

I want to begin by assuring the Committee that the Privacy Office is engaged with Assistant Secretary Allen and his staff, our colleagues in the Office for Civil Rights and Civil Liberties, and with the Office of the Director of National Intelligence's (ODNI) Civil Liberties Protection Office to ensure the NAO will operate transparently and in full compliance with all statutory and policy requirements, including privacy. As the NAO develops, we will continue to identify privacy risks and fashion protections to mitigate or eliminate those risks. The NAO prioritizes the protection of privacy and civil liberties. All activities of the NAO fall under existing legal authorities, including Executive Order 12333 and the Privacy Act. I want to stress, as the program stands today, there has been no collection, use or maintenance of records about individuals as covered under the Privacy Act. Moreover, the Privacy Impact Assessment (PIA) of the NAO undertaken by my office and Mr. Allen's staff identified that the necessary safeguards where in place on the processes of the NAO providing appropriate privacy protections. Of course, we will continue to work with the NAO to see NAO continues to establish and maintain privacy protections throughout the development and implementation of this new effort, and we will be vigilant in our oversight responsibilities to ensure continued compliance with privacy law and Federal policies regarding the collection, use, maintenance, and dissemination of records.

The Privacy Office Interaction with Intelligence and Analysis

The Privacy Office believes it is never too early for a component or program to engage our office. Programs operate effectively and privacy interests are best served when privacy protections are considered in the earliest stages of program or system development. We call our efforts to embed privacy into Departmental programs in the earliest stages "operationalizing privacy." Frequent privacy training – at the time of hire and annually thereafter – active involvement in the technology investment review process, and issuance of our Privacy Technology Implementation Guide are just a few examples of the tools the Privacy Office uses to encourage operationalizing privacy within the Department. The Government Accountability Office (GAO) acknowledged our gains in this important goal during its recent review of our office. Still, in an organization as large as DHS, one of our biggest challenges is keeping abreast of

individual programs in their very earliest moments of conception. We rely very heavily on components to seize upon the lessons of our outreach and notify us of their future plans, even if the contemplated use of PII is remote.

My staff became part of the NAO's Policy and Legal Working Group in November 2006. The purpose of this working group was, and is, to advise the Director of the NAO and the implementation planning team on issues related to the formation and anticipated operation of this new Departmental initiative. The Privacy Office's role in the group is to ensure strict compliance with all applicable privacy law and policies.

The most significant result of this initial, but limited, interaction was the issuance of the NAO Concept of Operations (CONOPS). The CONOPS commits the NAO staff to conduct their authorized functions effectively while ensuring that their activities affecting U.S. Persons are conducted in a manner that protects privacy and constitutional rights. The CONOPS further commits the Privacy Office, along with the Office for Civil Rights and Civil Liberties, to provide support and guidance to the NAO, and recommend steps to reconcile the need to use domestic information with the keystone requirement of protecting the privacy and civil liberties of U.S. persons. DHS will also assure any future updates to the NAO CONOPS are reviewed by the Privacy Office in accordance with Privacy Office guidance. The governance structure calls for the DHS' Director of Operations Coordination to review the program annually, including its compliance with privacy requirements, and includes our offices and our colleagues at the ODNI Civil Liberties Protection Office as advisors to the National Applications Executive Committee.

The Privacy Office became more involved with NAO during the iterative PIA process. I&A and the Privacy Office worked together for several months to draft a PIA cataloging and documenting both potential privacy risks and the steps the Department will take to mitigate these risks.

The NAO Privacy Impact Assessment

The *E-Government Act of 2002* requires agencies to conduct a PIA when developing or procuring IT systems or projects that collect, maintain, or disseminate information in an identifiable form or about members of the public. The Department has pioneered the use of PIAs beyond what the E-Government Act requires in two ways which are relevant to our work with the NAO.

First, the Privacy Office recognized that privacy can be impacted by offices, such as the NAO, policies, and rules of the Department, in addition to information technology. Therefore, as a matter of policy the Privacy Office conducts PIAs to examine these offices, policies, and rules, as well, even though it is not required to under the E-Government Act. These PIAs examine the application of the Fair Information Practice Principles (FIPPs) to the policy or, in this case, the office. The eight FIPPs are rooted in

the tenets of the Privacy Act and govern the appropriate use of personally identifiable information (PII) at the Department.[1] They are:

1. Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system whose existence and purpose is a secret.

2. Individual Participation: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

3. Purpose Specification: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used and shared.

4. Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

5. Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department is limited to purposes compatible with the purpose for which the PII was collected.

6. Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

7. Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

[1] The Department's PIA Guidance defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department." Section 208 of the E-Gov Act requires agencies to conduct a PIA for systems which collect, maintain, or disseminate information in an identifiable form, which is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." (P.L. 107-347)

Second, as a matter of policy, the Privacy Office conducts PIAs on national security systems, which are exempted from the requirement under Title II of the E-Government Act (Section 202(i)); although, consistent with the need to protect the processes associated with national security, the Privacy Office refrains from publishing these PIAs on our public facing website, www.dhs.gov/privacy.

This broad use of the PIA beyond the strict requirements of the E-Government Act is consistent with the Privacy Officer's authority under Section 222 of the *Homeland Security Act of 2002* to assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information. We have found that PIAs are an invaluable tool for programs to understand how their use of information impacts privacy. In addition, PIAs enhance the confidence the public has in the steps DHS takes to protect privacy. Thus, I was pleased to see GAO report that our office had made significant progress in both the number and quality of PIAs issued by the office.

On June 15, 2007, the Department issued a PIA for the NAO. I&A shared it with various Congressional Committees, and I know this Committee has now seen it as well. The document is For Official Use Only and, therefore, was not made public – and I am limited in what I can say about it here. Nonetheless, the PIA examined the application of the FIPPs to the NAO as it is presently planned. At this time, privacy concerns are nominal because the NAO does not presently anticipate routinely using or maintaining PII. Should this change, all notice, comment and oversight requirements imposed by the Privacy Act, the Privacy Office, and, I'll add, the DHS Office for Civil Rights and Civil Liberties, will be strictly followed. This PIA, like every other issued by the Department, will be updated as often as is required. In fact, we anticipate issuing a new version of the PIA soon incorporating additional views; when the revision is complete, we will of course share it with this Committee.

Finally, I want to note that in order to improve our ability to conduct privacy oversight for I&A, Privacy Office staff, including the Chief Privacy Officer, are undergoing training on intelligence law and the intelligence community, to better understand that community's mission and legal constraints. The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, the "Church Committee," and the report of the Rockefeller Commission, are all required reading in our office. We are mindful of the abuses of the past and we are determined that those abuses not be repeated at our Department.

The Privacy Office and Office for Civil Rights and Civil Liberties and ODNI's Civil Liberties Protection Office

I am particularly pleased to be appearing today with the Officer for Civil Rights and Civil Liberties, Dan Sutherland. His office and mine share a statutory obligation to work

together to ensure programs, policies and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner.

Both Mr. Sutherland and I have strived to give maximum effect to this statutory obligation. In addition to our frequent consultation, our staffs have instituted bi-weekly calls to ensure the close level of cooperation contemplated by the Homeland Security Act. The NAO is another opportunity for our offices to work together and coordinate our policies relating to privacy and civil rights and civil liberties.

Our office has developed a very close working relationship, as well, with our colleagues at the ODNI's Civil Liberties and Protection Office, which is charged with ensuring appropriate protections for privacy and civil liberties are incorporated in the policies and procedures of elements of the intelligence community within the National Intelligence Program, including DHS. I am pleased to be appearing today with Mr. Joel, who heads the ODNI's Civil Liberties Protection Office.

Our combined efforts on training and oversight will be critical to the success of the NAO.

Conclusion

The Privacy Office is committed to ensuring the NAO will be a success, both in terms of forwarding the critical missions of the Department and the United States Government to ensure the safety and well-being of our citizens, and equally in preserving the privacy protections the American public has a right to expect. I believe the NAO will not only preserve, but strengthen, these privacy protections.

This will require close cooperation between my office, the Office for Civil Rights and Civil Liberties, Assistant Secretary Allen and his staff, the Privacy and Civil Liberties Oversight Board, and the Office of the Director of National Intelligence. Together we will provide guidance, train staff and program participants, facilitate outreach with the privacy and civil liberties advocacy community, and exercise our oversight role zealously. We will continue to monitor the evolution and operation of the NAO to ensure the use of PII is done so in accordance with all applicable laws and policies. We will update the PIA as necessary, and will, of course, be happy to report our findings back to this Committee at any time.

I thank the Committee for this opportunity to testify about the NAO and its privacy compliance documentation, as well as the Privacy Office's role in moving the program forward successfully. I look forward to answering your questions.

Follow Up Address

Hugo Teufel III,
Chief Privacy Officer
U.S. Department of Homeland Security
Washington, DC 20528-0550
703-235-0780

Mr. Teufel's statement contains a brief history of the Privacy Office's engagement with the Department's planned National Applications Office (NAO), including the issuance of a Privacy Impact Assessment, as well as a discussion of the continuing efforts of the Privacy Office to ensure personally identifiable information is used by the NAO in accordance with all Federal privacy laws and policies.