WRITTEN STATEMENT

OF

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

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

FOR A HEARING ENTITLED,

"OVERSIGHT HEARING ON THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD AND THE DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICER"

JULY 24, 2007

Introduction

Chairman Sánchez, Ranking Member Cannon, and Members of the Subcommittee, 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 review of our office by the Government Accountability Office (GAO). I am particularly pleased to be testifying at a hearing with Alan Raul from the Privacy and Civil Liberties Oversight Board (PCLOB). I have known Alan for a number of years and my office works closely with PCLOB on privacy issues.

Because this is my first time appearing before the Subcommittee, I would like to introduce myself. 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, and disclosure of personal information; assuring that the Department complies with fair information practices as set out in the Privacy Act of 1974; conducting privacy impact assessments 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 Congress receives appropriate reports on such programs, policies, and procedures; and preparing an annual report to Congress on the activities of the Department that affect privacy. Additionally, I am responsible for overseeing DHS' implementation of privacy-related regulations and policies.

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

In April 2007, the GAO issued a report entitled, "DHS PRIVACY OFFICE: Progress Made but Challenges Remain in Notifying and Reporting to the Public." This review constituted GAO's first-ever review of the DHS Privacy Office following the creation of the Department. When the Privacy Office stood up four years ago, it took on the unprecedented responsibility of a systematic review of both nearly 300 systems of records and many hundreds of information technology systems that were either part of the legacy agencies or incorporated into new components. Since starting with two people, the Privacy Office has grown in size and, through investment in personnel and hard work, created a comprehensive process to ensure privacy is protected when personally identifiable information (PII) is used or disclosed by DHS.

"Significant" and "Substantial" Progress

I was gratified to see that GAO acknowledged the Privacy Office has made "significant progress" in reviewing and approving Privacy Impact Assessments (PIAs). PIAs are required for certain systems under the E-Government Act, and are an invaluable

tool programs use to understand how their use of information impacts privacy. They are so useful, in fact, that we made a policy decision to complete a PIA for many programs under the authority of Section 222 of the Homeland Security Act, even when one is not required under the E-Government Act. In addition to helping programs identify and mitigate privacy concerns, PIAs also enhance the confidence the public has in the steps DHS takes to protect privacy; PIAs required by the E-Government Act are available for review on the Privacy Office's public facing website, www.dhs.gov/privacy.

I am pleased to report that our office is increasing its capacity to conduct PIAs. In FY05, the Privacy Office conducted approximately 17 PIAs; in FY06, that number rose to 25; and in the current fiscal year, we've already conducted 42 PIAs. While this marked increase is cause for satisfaction, it must be noted that the quality of PIAs increased significantly over this time as well. So reported GAO; and on this point, we concur.

This high standard is the result of regular refinement of the Privacy Office's PIA Guidance. In its report, GAO mentioned two updates to the PIA Guidance. In May 2007, after GAO published its report, the Privacy Office issued a new version of the PIA Guidance. The Privacy Office's Director of Compliance introduced these changes at a PIA workshop attended by more than 100 individuals. The next PIA workshop will be offered together with training for privacy incidents involving PII at the DHS annual Security Awareness Training conference in late summer 2007. I am confident that these efforts will support the trend of simultaneous increases in the number and quality of PIAs issued by the Department.

I was equally pleased to see in the GAO report that the Privacy Office has taken steps to integrate privacy into DHS decision-making. We term this important goal "operationalizing privacy." To achieve this, the Privacy Office forms close relationships with system owners and program managers, along with IT security officials, and senior DHS officials. By placing privacy into the program development and decision-making processes of the Department, we can ensure that DHS not only meets its legal requirements and improves the effectiveness of the Department's programs, but stands as a model of how privacy can complement and work with law enforcement and intelligence agencies.

As part of our ongoing operations, our Compliance group works with IT security, budgeting, procurement, financial, and program professionals Department-wide to complete Privacy Threshold Analyses (PTAs), PIAs, system of records notices (SORNS), and other privacy documentation relevant to and required for DHS' systems and programs.

GAO Recommendations

GAO made four recommendations to improve the Privacy Office's effectiveness:

(1) Designate full time privacy officers at key DHS components, such as Customs and Border Protection, the U.S. Coast Guard, U.S. Immigration and Customs Enforcement, and the Federal Emergency Management Agency.

(2) Implement a department-wide process for the biennial review of system or record notices, as required by OMB.

(3) Establish a schedule for the timely issuance of Privacy Office reports (including annual reports), which appropriately consider all aspects of report developmental clearance.

(4) Ensure that the Privacy Office's Annual reports to Congress contain a specific discussion of complaints of privacy violations, as required by law.

GAO provided the Privacy Office with a draft of its report, and our reply appears as an attachment to their final report. While this is a matter of public record already, I will summarize our reply and review the steps the Privacy Office has taken to implement the recommendations.

Recommendation One – Designate full time privacy officers at key DHS components, such as Customs and Border Protection, the U.S. Coast Guard, U.S. Immigration and Customs Enforcement, and the Federal Emergency Management Agency.

The Privacy Office recognizes a strong correlation between the designation of privacy officers at the component and program level, and the success of the Privacy Office's mission within those components and programs. Privacy officers at the Transportation Security Administration and the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program office, for instance, are an important factor ensuring privacy is operationalized. While GAO observed that the components with designated privacy officers have produced a majority of the PIAs issued to date, this is just one example of the important contribution these component privacy officers make in embedding privacy into departmental programs. These component privacy officers provide day-to-day privacy expertise within their components to programs at all stages of development, ensuring that privacy is considered from the design through the implementation phase of every program within their component.

This recommendation is consistent with DHS Privacy Act Compliance Management Directive (MD) No. 0470.2. Specifically, section V.B.1. of the MD directs Under Secretaries and all DHS Designated Officials to:

Appoint an individual with day-to-day responsibility for implementing the privacy provisions of the Privacy Act, and any other applicable statutory privacy requirement.

The Privacy Office will continue to press the importance of placing privacy officers within the components and work with the Department to develop position descriptions and provide necessary training to support this development. We are working with senior leadership of the Department to designate component privacy officers in components that make significant use of PII.

Recommendation Two - Implement a department-wide process for the biennial review of system-of-records notices, as required by OMB.

The Privacy Office concurs with this recommendation. The Privacy Office developed the PTA in order to understand which nascent systems at DHS handle or involve PII and, of those systems, which need PIAs. Based on the analysis of the PIA, the Privacy Office can then identify which systems need new or updated SORNs. The Privacy Office found that the most expedient process to ensure overall privacy compliance focuses first on the development of the PIA and then on any the corresponding SORN, because the PIA helps identify the appropriate purposes, routine uses for disseminating information, types of information, categories of individuals affected, and, if applicable and appropriate, exemptions from certain Privacy Act requirements for the system of records.

The Privacy Office developed a two prong approach to reviewing the legacy SORNs and updating them appropriately. As noted in the GAO report, the Privacy Office has a well-developed PIA compliance process. Part of that process identifies the legacy SORNs and determines whether an updated or new SORN must be published. Next, the component, the Privacy Office, and the DHS Office of the General Counsel

review the SORN to issue a DHS SORN that is updated appropriately to describe the program as it exists under DHS and its homeland security mission. Programs making operational enhancements may not implement any updates until DHS publishes the SORN in the *Federal Register* and the Privacy Office approves the PIA.

In the second prong of the SORN review, the Privacy Office is systematically reviewing, by component, the legacy SORNs in order to issue updated SORNs on a schedule that prioritizes those systems with the most sensitive PII.

As of July 2007, the Privacy Office holds 266 System of Records, of which 215 are legacy system of records. DHS has issued 55 notices for updates to system of records, new system of records, and retirement of existing system of records. DHS is actively reviewing its remaining legacy system of records.

By the end of FY 2007, the Privacy Office will issue an updated System of Records Notice Guide to help in the drafting process. The Privacy Office is also developing a library of acceptable routine uses that components can use to identify appropriate routine uses as they review and develop their own SORNs. This will likely reduce the time needed to review draft SORNs.

This two-pronged approach will permit the Privacy Office to work with DHS components to evaluate methodically, and in a timely fashion, all of the existing SORNs to determine if the need exists to re-issue, remove, or re-draft each notice. The Privacy Office has met with a number of components and will meet with all others to establish appropriate timelines to accomplish this goal, consistent with the Privacy Office's responsibilities under issued OMB guidance.

Recommendation 3 – Establish a schedule for the timely issuance of Privacy Office reports (including annual reports), which appropriately consider all aspects of report development including departmental clearance.

The Privacy Office concurs and fully acknowledges the need for the timely issuance of its reports, including its annual report, and applies full effort to meet any report deadlines. The Privacy Office will work those components and programs impacted by its reports to provide for both full collaboration and coordination within DHS and timely issuance of its reports. We are confident that our reports will be timelier in the future. Our next annual report will cover the period from July 2006 to July 2007, and will soon be completed and sent to Congress.

On July 6, 2007, The Privacy Office released our 2007 Data Mining Report. This is exactly one year from the date of release of our 2006 Data Mining Report. The recent effort was not merely an update to the earlier report, however. We first had to familiarize ourselves with a new definition of "data mining" supplied in House Report No. 109-699 – *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes*. Then we had to apply that definition against all existing programs and new programs instituted throughout the year.

The last report I will mention here is the Privacy Office's review of the Science and Technology Directorate's Program, "Analysis, Dissemination, Visualization, Insight and Semantic Enhancement" (ADVISE). This report was initiated by me under the authority of Section 222 of the Homeland Security Act, which designates the Chief Privacy Officer as the DHS senior official responsible for ensuring that PII is used in full compliance with the fair information practices of the Privacy Act of 1974 and for reporting on complaints of privacy violations. As such, there is no statutory due date for

this report. Nonetheless, as GAO stated, giving the public and Congress timely information about programs supports transparency and accountability, two of the fair information practices the Privacy Office promotes. Accordingly, we are committed to issuing reports as quickly as is consistent with creating a useful, quality product. On March 21, 2007, I testified before the Homeland Security Subcommittee of the U.S. House of Representatives Committee on Appropriations. At that time, I answered a question about our efforts to review the ADVISE program. I stated that our review would be completed in a matter of weeks and that the report would be issued soon.

It is now four months later, and I wish to say a word about the interim. As it becomes clear reading the report, the term ADVISE covers a number of tools in various stages of development and use within several DHS components. To make sense of these after our initial review, we divided our examination into the ADVISE Technology Framework and the ADVISE Deployments, and proceeded to examine the privacy implications of each. This took longer than I anticipated it would during my March 21st testimony. Nonetheless, I believe the extra time it took to fully understand what we mean when we say "ADVISE" and then flesh out the privacy concerns with each will make the report much more informative and useful to the public, Members of Congress, and the Department programs planning to use ADVISE in the future.

> Recommendation 4 – Ensure that the Privacy Office's annual reports to Congress contain a specific discussion of complaints of privacy violations, as required by law.

While the Privacy Office acknowledges that Section 222 of the Homeland Security Act of 2002 requires the Privacy Office to include in its annual report to Congress a number of items of information, including "complaints of privacy violations,"

the Privacy Office interpreted this list as descriptive, rather than prescriptive, in terms of where this information appears in the report. As such, the last report noted the privacy complaints the Privacy Office received within the substantive discussion of the actions of the Privacy Office.

For example, in the section discussing the reports provided to Congress, the last annual report notes the *Report on the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties* and the 2006 *Data Mining Report*. Although both reports were completed in response to Congressional requests, they dealt with privacy issues that surrounded complaints received by the Department. Additionally, this annual report discussed the work on the *Secure Flight* and *MATRIX* reports, which have since been issued and were directly responsive to complaints received by the Privacy Office. Further, the annual report noted the work of the Privacy Office with regard to the Undertakings concerning Passenger Name Records (PNR) and REAL ID, issues that had generated a number of comments to the Privacy Office from privacy groups, if not specifically privacy complaints. Thus, throughout the last annual report, the Privacy Office noted issues of interest brought to its attention regarding privacy and DHS.

Nonetheless, the Privacy Office agrees that for the sake of clarity a consolidated reporting structure for privacy complaints within future annual reports will assist in assuring Congress and the public that the Privacy Office is addressing the complaints that it receives.

External, Interagency, and International Outreach

The Privacy Office mission extends beyond operationalizing privacy within DHS. We also undertake a number of outreach initiatives in order to enhance transparency with

the general public and increase understanding of what the Department does to protect privacy, share best practices, adhere to privacy law, and respect the fair information practices. I was pleased to see that many of our outreach initiatives were also favorably reported by GAO.

The Data Privacy and Integrity Advisory Committee

The DHS Privacy and Integrity Advisory Committee (DPIAC) is chartered to offer advice and guidance to the Secretary and the Chief Privacy Officer on programmatic, policy, operational, and technological issues within DHS that relate to PII, as well as data integrity and other privacy-related matters.

The DPIAC was formed under the Federal Advisory Committee Act (FACA) in 2004. Members come from large and small companies, academia, and the non-profit sector, and are selected because of their expertise, education, training, and experience in the fields of data protection, privacy, and/or emerging technologies. DPIAC meetings are open to the public, and generally they are well attended.

Since its first meeting in 2005, the DPIAC has issued six reports with a total of 36 recommendations to enhance privacy protection within the Department. The advisory committee has met three times in FY07, and at its last meeting issued a report entitled "Comments Regarding the Notice of Proposed Rulemaking for Implementation of the REAL ID Act." This report has been shared with the Department's REAL ID governance committee and is assisting the Privacy Office to evaluate the privacy issues related to the drafting and implementation of the final rule. Of course, this report and all other DPIAC reports are available on the Privacy Office's public website.

The next meeting of the DPIAC will be held in September in Washington, DC.

White House Privacy and Civil Liberties Oversight Board

The Privacy Office continues to have a close working relationship with the President's Privacy and Civil Liberties Oversight Board (PCLOB). The executive director, Mark Robbins, appeared before the DPIAC at its meeting on September 20, 2006 and provided a summary of the board's activities since its inception. He described the mission of the board, articulating three charges: to participate in the development, implementation, and review of the guidelines for the information sharing environment (ISE); to release an annual report to Congress; and to advise the President and senior executive branch officials on how to ensure privacy and civil liberties interests based on current law, regulations, and policies. He also answered a number of questions from the DPIAC members, making it an informative and useful session. I am pleased to tell you that my colleague, Dan Sutherland, Civil Rights and Civil Liberties Officer at the Department, and I meet and converse regularly with Mark and our privacy and civil liberties colleagues at other agencies. As well, the Secretary and I have briefed the Board on occasion as requested by the Board.

Information Sharing Environment

Section 1016 of Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) required the federal government to put into operation a recommendation of the 9-11 Commission to create a new means and methodology to share terrorism information across the entirety of the federal government as well as state, local, tribal, and foreign governments and private sector entities. Furthermore, the statute created the Program Manager's Office (PM/ISE) for the development and implementation of the ISE.

The DHS Privacy Office participated in all ISE Coordinating Group activities, providing necessary privacy leadership and supporting Departmental goals, and coordinated with other parts of the Department, including the Office of Security, the Office of the Chief Information Officer, and the Information Sharing & Collaboration Office. The output of these Coordinating Groups was used by the PM/ISE to respond to the President's direction, set out in a Presidential Memorandum dated December 15, 2005, setting forth specific guidelines and requesting recommendations for development of the ISE.

Out of these guidelines, specific working groups were developed with specified agency leads to provide specific guidance. The Privacy Office participated on a number of groups, including the Privacy group (Guideline 5), the Controlled Unclassified Information (CUI) group (Guideline 3), Foreign Government Information (FGI) group (Guideline 4), and participates in the State, Local, Tribal, and Private Sector group.

Privacy and Civil Liberties Committee

The Privacy Office participates in the interagency Privacy and Civil Liberties Committee co-chaired by OMB and the Department of Justice. This quarterly forum allows privacy personnel from all Federal agencies to exchange views and information on issues of mutual concern and discuss privacy best practices government-wide.

President's Identity Theft Task Force

Through Executive Order 13402, issued on May 10, 2006, the President established an Identity Theft Task Force comprised of 17 federal agencies, including DHS. The mission of the Task Force was to develop a comprehensive national strategy to combat identity theft. In the Executive Order, the President specifically directed the

Task Force to make recommendations on steps the federal government can take to reduce the likelihood of identity theft.

The Task Force recommended that OMB and DHS outline best practices in the arena of automated tools, training processes, and standards that would enable agencies to improve their security and privacy programs. In response to this recommendation, OMB and DHS developed a paper, titled "Common Risks Impeding the Adequate Protection of Government Information," which identifies common risks, or "mistakes," impeding agencies from adequately protecting government information. Agencies may refer to this paper, which is posted on the web sites for the Chief Information Officer (CIO) Council and the National Institute of Standards and Technology (NIST), when considering steps necessary for administering agency information security and privacy programs as required by law, policy, and guidance.

International Outreach

The Privacy Office provides crucial policy and programmatic guidance to the Secretary, Directorates and component agencies on international privacy matters. Over the past year, the Privacy Office has continued to expand both in its reach and in its effectiveness within the Department and with its partners abroad. The office expects this to continue throughout 2007 with more high profile cross-border data sharing issues facing the Department.

When the United States – European Union (U.S.–EU) Agreement on Passenger Name Records (PNR), in effect since 2004, was overturned by the European Court of Justice in May 2006, the DHS Policy Office led the negotiation of an interim agreement

and continues discussions with the European Commission. Because of the Privacy Office's expertise on international privacy frameworks, it became an important resource to the DHS negotiating team that successfully concluded a new PNR agreement.

In the last twelve months, the Privacy Office represented the U.S. government and DHS privacy policies at the following international forums: The International Conference of Data Protection and Privacy Commissioners in London, England; The Organization for Economic Cooperation and Development (OECD**)**; and the International Association of Privacy Professionals (IAPP) meeting in Ontario, Canada.

In September 2006, the Privacy Office made a presentation to the Asian-Pacific Economic Cooperation (APEC) E-Commerce Steering Group on the DHS development of Privacy Impact Assessments. The Privacy Office also led the drafting of privacy provisions in the Regional Movement Alert System, a counter-terrorism initiative to share lost and stolen passport information with foreign partners. The resulting Memorandum of Understanding was adopted as a model by the APEC Business Mobility Group and endorsed by the APEC Ministers.

The Privacy Office co-hosted an International Conference on Biometrics and Ethics with US-VISIT and the DHS Biometric Coordination Group, in late 2006, in Washington, DC. This conference was held to promote understanding and international cooperation on the use of biometrics as its technologies evolve and impact individuals' privacy. The conference brought together approximately 80 experts from several countries to engage in an open discussion of the application and ethics of biometrics. Participants included representatives from academia, private industry, non-profit organizations and government, and hailed from Asia, Europe, the Middle East and North

America. In addition to DHS, representatives from the U.S. Departments of Defense, Justice and State also attended.

In January 2007, the Privacy Office participated in the APEC E-Commerce Steering Group's (ECSG) Data Privacy Subgroup (DPSG) meeting in Canberra, Australia where participants agreed upon a model for the commercial cross-border exchange of PII. The Privacy Office remains engaged in APEC activities to ensure that the scope of discussions does not jeopardize data sharing in the national security/law enforcement context.

Later in January, the Director of International Privacy Policy (who was recently selected to be the Deputy Chief Privacy Officer) attended a two day conference on Aviation Security in Singapore. More than 50 officials from the aviation security branches of Asian, Canadian and Middle Eastern governments attended, along with private representatives from the aviation industry. The Director presented an overview of DHS and its use of personal information relevant to aviation security. He also discussed developments in the EU and Asia Pacific region and suggested a global strategy for resolving impediments to the free flow of information for law enforcement and national security purposes. The Director's participation set the foundation for further contacts with Singapore data protection officials, who expressed a willingness to share developments in their privacy work.

Most recently, the Privacy Office's Director of International Privacy Policy and I traveled to Brussels to meet with members of the international and European media as well as E.U. government officials that included the European Data Protection Supervisor;

members of the Freedom, Security and Justice Directorate of the Commission; and members of the European Parliament.

The Privacy Office has endeavored to reach overseas audiences and increase understanding of USG privacy policy through publication of articles in the Bureau of National Affairs Privacy & Security Law. In *The Golden Rule of Privacy: A Proposal for a Global Privacy Policy On Government-to-Government Sharing of Personal Information*, the Director of International Privacy Policy suggests an approach based on the Fair Information Practices combined with the basic international principle of reciprocity. The Privacy Office has also prepared *Accountability and Oversight in the U.S. System*, as well as *Notice and Consent Principles in International Guidelines, Agreements and National Legislation*, which will be published later in 2007.

Conclusion

I thank the Subcommittee for this opportunity to testify about the significant efforts of the Privacy Office. I and my office look forward to demonstrating continued improvement in our efforts to ensure privacy is protected throughout the Department of Homeland Security.