Annual Report

Privacy Office Annual Report to Congress

July 2004 – July 2006

Homeland Security

Privacy Office
Annual Report to Congress
July 2004 – July 2006

Privacy Office
U.S. Department of Homeland Security
Washington, DC

July 2006

Honorable Members of Congress:

I am pleased to present to Congress the Annual Report of the Privacy Office. This document covers two reporting periods: July 2004 through June 2005 and July 2005 through July 2006.

The first Privacy Office Annual Report covered the period from April 2003 through June 2004 and was issued on February 2005. The second Annual Report, covering the period from July 2004 through June 2005, was substantially complete when the Department's first Chief Privacy Officer, Nuala O'Connor Kelly, resigned to return to the private sector. The acting Chief Privacy Officer, Maureen Cooney, decided to merge this earlier report with the report for next reporting period. Unfortunately, Ms. Cooney retired from federal service before the Office was ready to release the combined report, which was substantially complete.

Further adding to the time it took to release the combined report was the need to ensure that the combined draft document had been reviewed for accuracy and completeness by the various stakeholders throughout the Department. After discussions within the Office, I decided that the best approach would be to put the document through the standard departmental review process. Although this additional review added time to an already overdue report, I am certain that the receipt and selected incorporation of stakeholder comments made for a better, stronger document. Importantly, the heavy lifting in preparing this document was borne by Ms. Kelly and Ms. Cooney. I commend them for their hard work, both on the report and within the Privacy Office.

July 2004 through July 2006 was a time of significant progress for the Privacy Office. The Office concentrated on developing an awareness of privacy from the top leadership to the officer at the border. As well, the Office worked to connect operational issues to tangible processes when evaluating appropriate privacy choices throughout the Department.

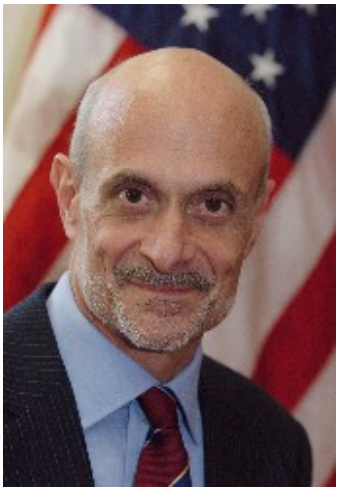
I look forward to continuing the good work of the Privacy Office here at DHS. I am certain that we at DHS can, and will, secure the Homeland while protecting privacy.

Respectfully submitted,

Hugo Teufel III
Chief Privacy Officer
U.S. Department of Homeland Security

Privacy and Protecting Our Homeland

Preserving our Freedoms, protecting America…We secure our homeland.



"The Department has the opportunity to build into the sinews of this organization, respect for privacy and a thoughtful approach to privacy. . . . If done right, it will be not only a long-lasting ingredient of what we do in Homeland Security, but a very good template for what government ought to do in general when it comes to protecting people's personal autonomy and privacy."

The Honorable Michael Chertoff
Secretary
U.S. Department of Homeland Security

TABLE OF CONTENTS

I. OVERVIEW OF PRIVACY ACTIVITIES

The mission of the Privacy Office is to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while achieving the mission of the Department of Homeland Security.

The Privacy Office will achieve its mission through:

- Internal education and outreach efforts to imbue a culture of privacy and a respect for fair information principles across the department.
- Constant communication with individuals impacted by DHS programs to improve our understanding of DHS's impact, and, where necessary, modify DHS activities – through formal notice, constructive policy discussions, and complaint resolution mechanisms.
- Encouraging and demanding at all times an adherence to the letter and the spirit of laws promoting privacy, including the Privacy Act of 1974 and the E-Government Act of 2002, as well as widely accepted concepts of fair information principles and practices.

– Privacy Office Mission Statement

The Privacy Office has been working diligently to ensure that DHS programs enhance our nation's security while preserving our liberties. Consistent with the statutory mission set forth in Section 222 of the Homeland Security Act of 2002, the Privacy Office has continued to foster a culture of privacy in the Department throughout the period of July 2004 – July 2006, helping managers and strategists within DHS build compliance with fair information principles into programs that fulfill the Department's homeland security mission.

This report covers management of the Privacy Office under former Chief Privacy Officer Nuala O'Connor Kelly and former Acting Chief Privacy Officer Maureen Cooney and is set out in five parts. Parts I and II provide an overview of many of the activities of the reporting period, including a focus on the legislative activities relevant to privacy and homeland security that have shaped particular areas of work. Part III focuses on how the Privacy Office's work has been integral to the overall success of the DHS mission. Part IV describes how the office has responded to a wide array of changing circumstances, both nationally and globally, including significant new Presidential Directives, and responses to terrorist threats. Part V sets out the challenges and opportunities for the upcoming year.

The Privacy Office is proud of its accomplishments, which could not have been achieved without the support of DHS Secretaries Ridge and Chertoff, our partners throughout the Department, other Federal agencies, the international community, Congress, and the American public.

A. Operationalizing Privacy

Operationalizing privacy has been at the core of all Privacy Office efforts -- that is, seeking full implementation of the fair information principles, as embodied in the Privacy Act, as well as compliance with the E-government Act of 2002, the Federal Information Security Management Act (FISMA) and disclosure responsibilities under the Freedom of Information Act (FOIA).

The Privacy Office will continue its work to ensure that individual programs sustain and enhance privacy protections through its general Privacy Impact Assessment (PIA) and Systems of Record Notice (SORN) review process, as well as through its role in the Office of Management and Budget's OMB 300 Privacy Impact Assessment reviews and throughout the technology lifecycle review processes. Throughout this past year, the Privacy Office worked even more closely with the Office of the Chief Information Officer (OCIO) to build additional privacy protections into systems used across DHS. The office also worked with the Science and Technology (S&T) Directorate to add privacy protections into the approval process for new

research initiatives. These two initiatives are intended to place privacy at the front end of planning and development for DHS information technology.

PIAs are fundamental in making privacy an operational element within the Department. Conducting PIAs demonstrates the Department's efforts to assess the privacy impact of utilizing new or changing information systems, including attention to mitigating privacy risks. Touching on the breadth of privacy issues, PIAs allow the examination of the privacy questions that may surround a program or system's collection of information, including commercial reseller data as well as the system's overall development and deployment. When prepared early in the development process, PIAs provide an opportunity for program managers and system owners to build privacy protections into a program or system in the beginning. This avoids forcing the protections in at the end of the developmental cycle when remedies can be more difficult and costly to implement.

In accordance with Section 208 of the E-Government Act of 2002, the Department of Homeland Security is required to perform PIAs whenever it procures new information technology systems or substantially modifies existing systems that contain personal information. Although the E-Government Act allows exceptions from the PIA requirement for national security systems, DHS is implementing Section 222 of the Homeland Security Act to require that all DHS systems, including national security systems, undergo a PIA if they contain personal information. The Privacy Office has staff with security clearances that allow them to work with programs to assess the privacy impact of classified systems or systems that contain classified information. In cases where the publication of the PIA would be detrimental to national security, the PIA document may not be published or may be published in redacted form.

The Office has worked closely with DHS components to standardize the PIA process and to increase compliance with the PIA requirement. The Privacy Office updated and reissued its Privacy Impact Assessment Guidance in March 2006 and distributed it widely within the Department and to Federal partners. In June and July, PIA training was conducted for more than 500 Federal employees. The Privacy Office intends to continue to conduct outreach and training to enhance the Department's appreciation of the value of PIAs and to explore how privacy audits can provide greater accountability and compliance with privacy safeguards.

A significant part of the Privacy Office efforts has focused on the importance of transparent dialogues concerning Departmental operations and privacy issues of concern to DHS and across the Federal government. These have included the collection and use of commercial information, appropriate privacy protections for the information sharing environment, and topics as diverse as identity management and the impact of technologies such as biometrics and radio frequency identification on individual privacy within a security context.

The Privacy Office is also an integral member of the teams planning and implementing departmental programs that use personal information from non-DHS sources. Our role was particularly evident during our participation in the DHS Second Stage Review on screening programs. Additionally during this reporting period, the office provided specific guidance on privacy measures for the Secure Flight program, conducted a comprehensive review of the implementation of the arrangement to transfer Passenger Name Record (PNR) information from air carriers in the European Union (EU) to the Bureau of Customs and Border Protection (CBP), and analyzed and advised on privacy issues concerning data governance and data security. Most recently, the Privacy Office has partnered with the OCIO to provide guidance on privacy protection through data security within DHS and in terms of best practices in the Federal space, working with interagency partners and supporting the President's Identity Theft Task Force. We expect work in each of these areas to be ongoing and in partnership with many other DHS components and offices.

B. Reports to Congress

The Privacy Office delivered two major reports to Congress, a *Report on The Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties, as Required under Section 4012(b) of The Intelligence Reform and Terrorism Prevention Act of 2004* (April 27, 2006) and a *Data Mining Report* (July 6, 2006), as required by the Department's Appropriations legislation. Earlier, in September 2005, we also published a substantial *Report Concerning Passenger Name Record Information Derived from Flights Between the U.S. and the European Union* (September 19, 2005), about which we briefed Members extensively.

Additionally, since 2004, on a quarterly basis, we have distributed to all Members of Congress the Privacy Office newsletter, *Privacy Matters*, providing periodic updates on Privacy Office and Department-wide privacy activities. We conducted programmatic reviews of the Multistate Anti-Terrorism Information Exchange (MATRIX) and Secure Flight programs. With respect to privacy and technology, Privacy Office staff substantially led and developed the Federal government report *Privacy and Biometrics Conceptual Foundation*, sponsored by the National Science and Technology Council (April 2006). Further, Privacy Office staff produced *Annual Reports* for 2004 and 2005 on FOIA operations at DHS and accomplished an initial departmental *Freedom of Information Act Program Assessment and Improvement Plan Report*, pursuant to *Executive Order 13392: Improving Agency Disclosure of Information* (July 2006).

C. Testimony Before Congress

During the reporting period, DHS Chief Privacy Officers testified before several Committees of Congress on a range of privacy issues on behalf of the Department.

In September 2004, Ms. Kelly appeared before the House Judiciary Committee's Joint Hearing of the Subcommittees on Commercial and Administrative Law and the Constitution to address the recommendations of the 9-11 Commission's Report on appropriate privacy safeguards to facilitate information sharing.

On April 4, 2006, Acting Chief Privacy Officer Maureen Cooney appeared before the House Judiciary Committee's Joint Hearing of the Subcommittees on Commercial and Administrative Law and the Constitution to address the subject of "*Personal Information Collection by the Government from Commercial Data Resellers.*"

On April 6, 2006, Ms. Cooney testified before the House Homeland Security Committee's Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment on the subject of "*Privacy and the DHS Intelligence Enterprise.*"

And on May 17, 2006, Ms. Cooney testified again at an oversight hearing before the House Judiciary Committee's Subcommittee on Commercial and Administrative Law to address the subject of "*Privacy in the Hands of the Government*" as it pertained to DHS and the efforts of the Privacy Office.

D. Privacy Outreach Workshop Series

During 2005-2006, the Privacy Office sponsored a privacy workshop series that was open to the public and sought both public participation and comment.

In September 2005, the Privacy Office held a two-day workshop on *Privacy and Technology: Government Use of Commercial Data for Homeland Security*.

In April 2006, the Privacy Office held a workshop on *Transparency and Accountability: The Use of Personal Information within the Government*.

And in both June and July, 2006, the Privacy Office held workshops, as well as training opportunities for DHS and other Federal staff, on *Operationalizing Privacy: Compliance Frameworks & Privacy Impact Assessments*.

Agendas, highlights and transcripts of those workshops may be found on the Privacy Office website: www.dhs.gov/privacy.

E. Privacy Advisory Committee Open Meetings and Privacy Guidance

To receive the benefit of external advice from citizen experts on privacy and with the support of both Secretaries Ridge and Chertoff, the Chief Privacy Officer sponsored the establishment of an external advisory committee, the Data Privacy and Integrity Advisory Committee ("DPIAC" or "Committee"), established under the procedures of the Federal Advisory Committee Act. The Committee of volunteers provides advice to the Secretary and the Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues relevant to DHS that affect individual privacy, data integrity, and data interoperability and other privacy-related issues.

Since April 2005, the Committee has held six public meetings in Washington and in various regions around the country in order to facilitate citizen accessibility and participation. Full transcripts of those meetings may be found at the Privacy Office's website, www.dhs.gov/privacy.

During the past ten months, the Committee delivered three advisory reports to the Secretary and the Acting Chief Privacy Officer. They include reports on 1) *The Use of Commercial Data to Reduce False Positives in Screening Programs;* 2) *Recommendations on the Secure Flight Program*; and 3) *Framework for Privacy Analysis of Programs, and Technologies and Applications*. Subcommittees of the full Committee are currently studying a range of other issues, including the use of commercial data for broader DHS programs and the privacy considerations attendant to radio frequency identification (RFID) technology in the context of particular homeland security programs. Initial working drafts of advisory papers on those topics continue to be discussed and refined by the Subcommittees at this time and are expected to be presented to the full Committee for consideration at future meetings.

F. International Outreach

Our international mission to establish trusted links with our foreign partners continues to contribute to the Department's overall mission and vision as it seeks to implement new information systems and international partnerships. 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 the next year to be an even more productive one, as a direct result of the additional resources that Congress authorized for FY 2006 to support the mission of this office.

II. HOMELAND SECURITY LEGISLATION AND PRIVACY

In July 2004, the 9-11 Commission released the report of its investigation into the events leading to the terrorist attacks of September 11, 2001. Many of the changes to intelligence and law enforcement structures recommended in the report were later codified in the Intelligence Reform and Terrorism Prevention Act (IRTPA). In addition, Congress enacted the REAL ID Act of 2005,[1] which sets minimum standards for drivers' licenses and identification cards to be accepted for Federal purposes in order to prevent the fraudulent issuance and use of such documents. The Chief Privacy Officer and the staff of the Privacy Office have provided guidance on implementing these important legislative initiatives.

A. 9-11 Commission Report

In July 2004, the 9-11 Commission released its public report of findings and recommendations related to the terrorist attacks of September 11, 2001. The report's analysis and recommendations had direct implications for privacy issues. For example:

> Exchanging terrorist information with other countries, consistent with privacy requirements, along with listings of lost and stolen passports, will have immediate security benefits. We should move toward real-time verification of passports with issuing authorities.[2]
>
> As the President determines the guidelines for information sharing among government agencies and by those agencies within the private sector, he should safeguard the privacy of individuals about whom information is shared.[3]

In her testimony before the U.S. House of Representatives Judiciary Committee Subcommittee on Commercial and Administrative Law, Ms. Kelly reflected on the report and concurred with the Commission's conclusion that "the choice between security and liberty is a false choice." The work of the Privacy Office, which views the protection of privacy as neither an adjunct to, nor the antithesis of, the mission of the Department, reflects this philosophy. Privacy protection is at the core of the Department's mission, as it must be at the core of the national mission to reform and improve anti-terrorism efforts.

Ms. Kelly noted that many of the 9-11 Commission's recommendations focused on the need to better integrate and coordinate the data collected for antiterrorism efforts. At the center of these efforts must be clear parameters for sharing information in a way that protects privacy. Establishing reasonable limits on access and embedding fair information principles in the information sharing environment will be important, not only because it will protect individuals, but also because it will engender the kind of trust in government that is necessary to achieve the cooperation of both the public and private sectors.

B. Intelligence Reform and Terrorism Prevention Act

During the reporting period, Congress enacted the IRTPA. This far-reaching statute contains a number of general provisions that affect privacy, and thus, have required guidance from the Privacy Office in keeping with the office's statutory mandate to ensure that the use of technology enhances and does not erode privacy protections. The creation of an information-sharing environment, for example, calls for comprehensive privacy protections in the exchange of personally identifiable information between agencies. The Privacy Office has played a leadership role in the continuing interagency development of appropriate privacy-sensitive guidelines for information sharing.

---

[1] Division B-REAL ID Act of 2005, the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. 109-13, 119 Stat. § 231, 302 (2005) (codified at 49 U.S.C. § 30301 note).

[2] The 9/11 Commission Report (New York: W.W. Norton & Company), 389.

[3] Id., 394.

Section 4012 of IRTPA required the Privacy Officer to prepare and submit to Congress the *Report to Congress on the Impact of the Automatic No-Fly and Selectee Lists on Privacy and Civil Liberties* (the No-Fly report) assessing the impact of the automatic selectee and no-fly lists on privacy and civil liberties. As part of this report, the Privacy Office was asked to make recommendations for practices, procedures, regulations, or legislation necessary to minimize adverse effects of these lists on privacy, discrimination, due process, and other civil liberties. In addition, the report discussed the implications of applying these lists to other modes of transportation and the effect that the implementation of recommendations would have on the effectiveness of using such lists to protect the U.S. against a terrorist attack.

The No- Fly report is an example of the policy advice sought from the Privacy Office by Congress. The report provides an extensive factual background on the automatic selectee and no-fly lists. The report discusses how these lists are used in current travel screening programs; describes the experiences of individuals who are correctly or erroneously identified as being on one of these lists; and identifies privacy and civil liberties issues raised by the use of these lists. The report concludes with a set of findings and recommendations dealing with the standards for automatic selectee and no-fly lists, including issues that could arise if the lists are used in transportation modes other than aviation; approaches to ensuring appropriate use of information collected for terrorist screening purposes; and appropriate mechanisms and venues for redress in cases of individuals who either were placed on the lists improperly or were misidentified as being on the lists.

The report concludes that, by embedding appropriate safeguards into anti-terrorism programs and by using personal information for limited, legitimate, and appropriate purposes, DHS can successfully perform its mission while protecting the privacy and civil liberties that are essential to the American way of life.

C. The REAL ID Act

Among its statutory responsibilities, the Privacy Office is responsible for conducting privacy impact assessments of proposed rules of the Department. In fulfilling this responsibility, the Privacy Office has actively participated in the DHS working group developing regulations to implement the REAL ID Act of 2005.

Title II of the REAL ID Act, "Improved Security for Driver's License' and Personal Identification Cards" requires DHS in consultation with the Department of Transportation and the States to issue regulations that set minimum standards for state-issued drivers' licenses and identification cards to be accepted for official purposes after May 11, 2008 – including accessing Federal facilities, boarding federally regulated commercial aircraft, and entering nuclear power plants. These REAL ID documents will include minimum security requirements, including the incorporation of specified data, a common machine-readable technology, and certain anti-fraud security features.

The Act sets forth minimum issuance standards for state-issued drivers' licenses and IDs including: (1) verification of presented information; (2) evidence that the applicant is lawfully present in the United States; (3) physical security of locations where the identification cards are produced; and (4) physical security of the licenses to prevent tampering, counterfeiting, and duplication of the identification cards for a fraudulent purpose. The Act also identifies what data must be included on the card; what documentation must be presented before a card can be issued; and how the states must share drivers' license information to prevent licenses from being issued from more than one state.

Concerns have been raised about the privacy of the personally identifiable information stored on the licenses and in the state motor vehicle databases. In response to these concerns, the Privacy Office participated in drafting and reviewing the Notice of Proposed Rulemaking as well as funding a contract to support exploring the creation of a state federation to implement the information sharing required by the Act but to do so in a privacy sensitive manner, including privacy protections not necessarily provided for in

the Act or its implementing regulations. The Privacy Office championed the need for privacy protections, including state privacy protections, regarding the collection and use of the personal information that will be stored on the REAL ID drivers' licenses and will continue to do so throughout the rulemaking process.

In a related item, the Privacy Office provided privacy policy guidance to the Department to supplement OMB's Memo 06-06, "Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD)-12," the Presidential Directive on Policy for a Common Identification Standard for Federal Employees and Contractors. The Privacy Office PIA Guidance was considered by OMB in developing the OMB HSPD-12 guidance.

III. BUILDING A CULTURE OF PRIVACY ATTENTIVENESS AT DHS

The Privacy Office performs a dual role for DHS. Internally, the office works to educate, inform, and create processes that reflect privacy and fair information principles in the evolution of all new agency programs, procedures, policies, and technologies, including the hiring and training of new personnel. Externally, the office reports to Congress on the activities of the Department that affect privacy. This dual role provides the benefit of a central, coordinating privacy authority within the Department that is knowledgeable about departmental organizational structures and is able to obtain necessary information, yet is independent so that it may act as an effective privacy advocate and a fair broker on complaints regarding various programs and within components.

This section of the report discusses the work of the Privacy Office within DHS and with other agencies of the Federal government.

A. Embedding Privacy

Embedding a culture of privacy within the Department requires the Privacy Office to work in partnership with others. Over the course of the reporting period, the Privacy Office has worked with the Office of the General Counsel (OGC) and the Office for Policy (Policy) on legal and policy issues; with various components on ensuring appropriate privacy education, training, and policies and procedures; with the Office for Civil Rights and Civil Liberties (CRCL) in areas where data use and protection intersected with civil rights issues; with the OCIO on matters related to building privacy into the DHS enterprise architecture and the system development lifecycle; with S&T on issues related to emerging technologies; and with the Information Sharing and Collaboration Office (ISCO) on privacy issues in the information sharing environment. This section elaborates on the Privacy Office's work within the Department.

1. Developing New and Reviewing Existing Systems of Records Notices

Compliance with the Privacy Act requires that each Department component maintaining personally identifiable information in a "system of records"[4] publish in the *Federal Register* a public System of Records Notice (SORN) describing the system. The Department includes both new and pre-existing components, and the Privacy Office is working with the components to review and update existing SORNs to assimilate and integrate all departmental record systems, eliminate duplicative systems, and ensure a consistent policy across the Department for using and sharing personally identifiable information.

The Privacy Office provides DHS components with basic guidance on drafting SORNs and standard language for routine uses to incorporate as necessary into such notices. These notices are then drafted by a program office and forwarded for review and clearance to the Privacy Office, with final review for compliance with *Federal Register* standards by the OGC. The SORN process provides the Privacy Office with a valuable opportunity to foster a culture of privacy within the Department and to ensure transparency for DHS operations that use personal information. Since the incorporation of all components on March 1, 2003, the Department has published 28 new or revised SORNs.

Reviewing and revising these Privacy Act notices constitutes the "bread and butter" of the Privacy Office. Because DHS programs must evolve to meet existing security threats and comply with legislative requirements, Privacy Act Notices necessarily remain a regular and ongoing part of the Privacy Office's work. Additionally, the drafting and reviewing of SORNs is a significant part of our statutory obligation to

[4] A "System of Records" is defined in the Privacy Act as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."
5 U.S.C. § 552a(a)(5).

ensure that the Department maintains personally identifiable information in conformity with the Privacy Act.

2. Reviewing IT Budgets and Privacy Impact Assessments

In order to effectively manage the Federal government's capital assets, OMB requires information technology (IT) projects seeking funding to submit a Capital Asset Plan and Business Case for approval. This plan, known as Exhibit 300, must demonstrate that the handling of personal information is consistent with relevant government-wide and agency policies. In many cases, as required by Section 208 of the E-Government Act, a PIA must be submitted to OMB along with the budget request.

The PIA document must answer the following questions, among others:

- What information is to be collected?
- What is the purpose or intended use of the information?
- With whom will the information be shared?
- What opportunities will individuals have to decline to provide the information or to consent to particular uses?
- How will the information be secured?
- Will a system of records be created under the Privacy Act of 1974?

Because a PIA is performed early in the development of a system and at every significant modification, it is a highly effective tool for identifying and mitigating privacy risks and embedding privacy into programs and systems. The Privacy Office has used PIAs as a focal point for its compliance activities. In its role as a partner to the departmental components, the office works closely with appropriate staff within components and directorates to complete PIAs. To increase the compliance rate and to increase understanding of the requirements and processes related to the PIAs, the office has provided PIA training to component and directorate system analysts, program managers, and budget managers. Over the past two years, the office has published updated guidance that reflects its experience with the PIA process.[5]

During fiscal year 2005, the Privacy Office began working with the OCIO and the Chief Financial Officer to review all IT budget submittals for compliance with OMB privacy requirements. Projects that did not sufficiently address privacy were not submitted to OMB.

From June 2004 through September 2005, the Privacy Office reviewed approximately two dozen IT budget submissions for Fiscal Year 2006 and 71 budget submissions for Fiscal Year 2007. During this time, the office determined that 54 PIAs were required. Between June 2004 and July 31, 2006, 44 PIAs were approved and published.[6]

3. Reviewing for Privacy Compliance

Privacy compliance reviews are another important tool for integrating privacy into departmental programs. The Privacy Office utilizes privacy compliance reviews to assess various aspects of the component's compliance, to provide input on the component's data protection practices, and to offer guidance on improving processes, policies, and systems.

---

5 PIA guidance can be found in the Privacy Impact Assessment section of the Privacy Office website: www.dhs.gov/privacy.

6 A complete list of published PIAs can be found in the Privacy Impact Assessment section of the Privacy Office website: www.dhs.gov/privacy.

The Privacy Office initiated its first privacy audit during the period covered by this report. The review involved implementation of the PNR Undertakings by CBP, dated May 11, 2004. The Undertakings were provided to the European Commission (EC) to facilitate a finding that adequate privacy protection would be provided to PNR data transferred by air carriers in response to U.S. government legal requirements. The Undertakings specify permissible uses of PNR data, the number and type of data elements that CBP may receive from airline reservation systems, data retention periods for different types of records, limitations on access to PNR data, the passengers' ability to request and ask for correction of their data, and the role of the DHS Chief Privacy Officer as the appeal authority with respect to these processes.[7] The Undertakings also specify that DHS and EC representatives will conduct a Joint Review to evaluate CBP's implementation of the Undertakings.

The Privacy Office conducted a compliance review in preparation for the Joint Review with the EC. The compliance review took place over the course of several months and consisted of a full analysis of CBP policies and procedures, interviews with key management and staff who handle PNR, and a technical review of CBP systems and documentation. During the course of the review, CBP made changes to various elements of its systems and to its policies, procedures, and guidance. Some of these changes were made unilaterally, as CBP found opportunities to improve its information practices. Many changes were the result of Privacy Office guidance. In some cases, the Privacy Office requested remediation, which CBP implemented. As a result of this constructive interaction, CBP achieved full compliance with the representations in the Undertakings and was prepared for the Joint Review.[8]

It should be noted that the European Court of Justice has nullified the PNR arrangement on the basis of a lack of proper legal foundation by the Council and EC for approving the agreement: thus, as of September 30, 2006, the arrangement was set aside by the Europeans. As of October 2006, the U.S. and E.U. concluded an interim arrangement that will be in effect until July 31, 2007.

4. Guiding Privacy Protective Identity Management

OCIO staff approached the Privacy Office for assistance with developing the DHS Identity Management initiative intended to establish a Departmental Identity Management and Access Control (IdM) mechanism. IdM is a set of business processes and supporting infrastructure enabling the secure sharing of information as part of a nationwide Terrorism Information Sharing Environment. IdM associates information access privileges with established credentials that may, in turn, be used to ensure "need-to-know" access to various applications.

The Privacy Office developed privacy protection guidance regarding the overall strategy and framework for the identity management initiative and worked closely with the OCIO to integrate this guidance into the planning phase of the IdM.

5. Instituting the DHS Data Integrity Board

Every agency that conducts or participates in a computer-matching program[9] is required by the Privacy Act to establish a Data Integrity Board. The board must approve all matching agreements in which

[7] The full text of the Undertakings can be found in the International Activities section of the Privacy Office website: www.dhs.gov/privacy.

[8] The Privacy Office report on its findings and recommendations, as well as other documents related to the Joint Review, can be found on the Privacy Office website: www.dhs.gov/privacy.

[9] A matching program is a computerized comparison of two or more automated systems of records or a comparison of a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance payments under Federal benefit program, or recouping payments or delinquent debts under such Federal benefit programs. 5 U.S.C. § 552a(a)(8).

the agency participates. The Secretary delegated this responsibility to the Chief Privacy Officer, who then quickly moved to establish the Data Integrity Board, composed of representatives from all DHS components, the Office of the Inspector General, the OCIO, and the OGC. The board also fulfills a second function by providing a forum to discuss ideas about privacy policy and responsible information management throughout DHS.

The board held several meetings during the reporting period. At its inaugural meeting, it established a subgroup to fulfill the Data Integrity Board requirements for the Department, chaired by the Chief Privacy Officer. This subgroup is responsible for reviewing and approving departmental matching agreements and approved a matching agreement between the United States Citizenship and Immigration Services (USCIS) and the Department of Education. Most DHS matching agreements involve USCIS and the agencies using its Systematic Alien Verification for Entitlements (SAVE) database to verify eligibility for benefits programs. During the past year, the board also approved a matching agreement concerning the Federal Emergency Management Agency (FEMA), to assist with information collection and sharing for purposes of disaster relief and public safety.

The larger Data Integrity Board worked with the Privacy Office to compile a list of DHS screening programs to assist the work of the DHS Data Privacy and Integrity Advisory Committee, and to assist the Privacy Office with FISMA's new privacy-related reporting requirements.

6. Providing Education and Training

Employee education and training is another tool for ensuring that privacy is embedded in the culture of the Department. The primary goal of privacy awareness training is to ensure that DHS employees are informed about how to handle personally identifiable information in a responsible and appropriate manner. To this end, in September 2004, the Privacy Office began conducting privacy awareness training for all headquarters employees. In addition to broad-based privacy awareness training, the Privacy Office conducted training on privacy impact assessment requirements for IT managers, business managers, and system analysts.

Additionally, to improve DHS employees' recognition of the privacy concerns that may occur within the course of their daily duties, the Privacy Office developed a new electronic learning course entitled *Privacy Awareness*. The course is a twenty-five to thirty-five minute interactive program reinforcing current privacy training for DHS employees and contractors on privacy awareness fundamentals. Additionally, the course gives a basic understanding of the privacy framework at DHS, each individual's responsibility, and the consequences for non-compliance with privacy policies. The use of scenarios in the course strengthens the understanding of the privacy objectives taught.

The Privacy Office has also begun designing two additional electronic learning courses entitled *Privacy Act 101* and *Privacy Act 201*. *Privacy Act 101* will amplify general employee knowledge of the Privacy Act of 1974. *Privacy Act 201* will educate supervisors about advanced business situations incorporating Privacy Act requirements. Furthermore, to supplement offline educational materials, the Privacy Office anticipates developing supplementary electronic learning courses regarding Privacy Impact Assessments, FOIA, and SORNs.

The Privacy Office updated and reissued its Privacy Impact Assessment Guidance in March 2006 and distributed it widely within the Department and to Federal partners. In June and July, PIA training was conducted for more than 500 Federal employees.

Departmental training augments employee training conducted by DHS components. Some components, such as the Transportation Security Administration (TSA) and CBP, require annual or bi-annual privacy awareness training for employees handling personal information. The United States Visitor

and Immigrant Status Indicator Technology (US-VISIT) program has also instituted mandatory privacy training for all employees and contractors with access to personal information.

7. Assisting with International Issues

Many of the Department's cross-border efforts involve information sharing and other data protection issues with foreign governments and regional organizations. For example, certain types of information sharing between the U.S. and the EU must address the terms of the 1995 European Directive on data privacy before they can be successfully implemented. Consequently, because of the office's expertise on international privacy frameworks, the Privacy Office is an important resource to DHS components whose operations extend beyond our borders.

In many cases, international issues are closely integrated with other activities within the Privacy Office. For example, the privacy compliance review of CBP's implementation of the PNR Undertakings and the subsequent Joint Review with the EC's representatives involved both privacy compliance and international expertise. The work on the Enhanced International Travel Security Initiative (EITS), described in detail later in this report, involves close collaboration between the Privacy Office staff with international expertise and with technology knowledge.

8. Providing Privacy Protection within DHS Components

While the Privacy Office provides departmental privacy policies and guidance, implementation takes place within the operating components. Some of the components – TSA, USCIS, and US-VISIT – have their own privacy officers responsible for compliance activities within their components and for coordinating with the Privacy Office. The office also has designated points of contact with CBP, USCIS, the Office of Intelligence and Analysis, and the United States Coast Guard (USCG). Components for which the Privacy Office recommended the designation of a privacy officer have included CBP, FEMA, Immigration and Customs Enforcement (ICE), and USCG. Due to the nature and high volume of programs initiated and carried out by these active components, and their direct interface with the public, the addition of a privacy officer or component privacy office that would look at the consistency of privacy policy implementation, best practices and staff training, rather than solely legal privacy compliance, would be of great value in achieving privacy and information governance synergies across the Department.

This section of the report discusses component- and program-based privacy activities.

a) The Transportation Security Administration (TSA)

The TSA privacy officer, now titled the Director of Privacy Policy and Compliance, is responsible for the agency's compliance with applicable privacy authorities and policies in coordination with TSA offices and the Privacy Office. The TSA privacy officer is also responsible for training employees on privacy laws, regulations, and policies; and for establishing systems to communicate its privacy policies to the public.

The TSA privacy officer, in coordination with the TSA Office of Chief Counsel, developed and implemented requirements for information sharing. Specifically, TSA deployed a chain-of-custody arrangement for PNR and a memorandum of understanding for sharing of terrorist information with the Terrorist Screening Center. TSA is also conducting a voluntary Registered Traveler pilot program with the Greater Orlando Aviation Authority that involves the provision of personal information in order for TSA to conduct security threat assessments on Registered Traveler pilot participants.

TSA seeks to incorporate privacy principles into the agency's systems development lifecycle and security architecture and into its program-based privacy impact assessments. During the past year, TSA has taken significant steps to augment its professional privacy staff and to specifically hire privacy leaders to manage privacy implementation for major TSA programs.

b) The National Cyber Security Division (NCSD)

The NCSD was created in June 2003 to serve as a national focal point for cyber security and to coordinate implementation of the *National Strategy to Secure Cyberspace*. To carry out its mission, NCSD has identified two overarching priorities: building an effective national cyberspace response system and implementing a cyber risk management program for critical infrastructure protection, including protection of key resources.

To increase situational awareness of government cyberspace and to monitor government agencies' information systems, NCSD developed the US-CERT EINSTEIN Program, administered through its branch U.S. Computer Emergency Readiness Team (US-CERT). While the program does not create a new system of records, it published a PIA on US-CERT EINSTEIN.[10]

Currently, along with the OCIO, the Privacy Office is working closely with NCSD on government sector security protocols to safeguard personal information collected, stored, and maintained on computer information systems.

c) The United States Citizenship and Immigration Services (USCIS)

USCIS designated a privacy officer for the component to work with the Privacy Office in March 2005. USCIS is the custodian of over 50 million records of aliens and immigrants who have entered this country. In the post-9/11 world, there is a growing demand for sharing the data contained in USCIS Alien ("A") files with Federal, state, and local law enforcement entities and other government agencies. DHS's challenge and responsibility is to protect the privacy interests of those individuals, while meeting the needs of law enforcement and benefit agency personnel. The Privacy Office works closely with the various program offices responsible for maintaining records systems.

During the past year, with the Department's assistance, USCIS entered into, and updated, a Computer Matching Act Agreement with the Social Security Administration (SSA). Under the agreement, USCIS will electronically transfer nonimmigrant information to the Supplemental Security Insurance (SSI) program of SSA. The SSA will use this information to assist them in determining whether recipients of SSI benefits have met their residency requirements.

B. Screening

DHS plays a critical role in securing the homeland through its numerous screening programs. One aspect of its multi-layered security system is the screening of those who have occupational access to the transportation system and maritime sector, passengers, and those who cross our borders. Screening activities depend on collection and analysis of personal information, so it is essential that privacy protection measures are embedded in screening programs and that the implementation of these measures be closely monitored. In each of the programs described below, the Privacy Office provided guidance and close review in preparing privacy documents supporting the information collection practices. This is one of the office's most important functions.

1. Transportation Workers

During 2004, TSA implemented several screening programs for those whose occupations require access to the transportation infrastructure. The programs, tailored to meet specific needs of various sectors of the transportation system and maritime environment, include the Transportation Worker Identification Credential (TWIC) pilot program, the Alien Flight Student Program, the Hazardous Materials Endorsement

[10] The PIA for US-CERT EINSTEIN can be found in the Privacy Impact Assessment section of the Privacy Office website: www.dhs.gov/privacy.

Program, the Crew Vetting Program, Security Threat Assessment for Aircraft and Heliport Operators, and Security Identification Display Area (SIDA) and Sterile Area Workers.

In each of these programs, TSA collects personal information from individuals seeking access to sensitive materials or secure areas and then uses this information to conduct security threat assessments to determine whether these individuals pose a risk to transportation or national security. In some cases, the security threat assessment also identifies individuals who may be wanted for the commission of a crime in the U.S. or elsewhere, or who are currently in violation of U.S. immigration laws. In the TWIC pilot program, those employees who qualified were issued an electronic credential that confirmed their eligibility to access secure areas at maritime facilities or on vessels. The credential was tamper-resistant and included a biometric to confirm the identity of the credentialed user.

TSA published PIAs that meet the requirements of OMB guidance and DHS policy for the pilot testing of its screening programs. TSA also published a PIA of the Vetting and Credentialing Screening Gateway System to describe the hardware, software, and communications infrastructure systems supporting these screening programs. For the programs that are ready to transition from a pilot to full implementation, PIAs have been updated, as required, to provide as much transparency as possible, consistent with the security requirement of each program.

2. Airline Passengers and Registered Traveler/Known Traveler

TSA is piloting a dual approach to airline passenger screening. Under the Registered Traveler Pilot Program, individuals who voluntarily undergo a security threat assessment may obtain a credential that may allow them to go through a faster screening process at the airport. Those who do not wish to provide information for a security threat assessment will be screened through a new passenger screening program that will screen all domestic airline passengers.

In 2004, TSA successfully initiated and carried out five federally managed Registered Traveler pilots, which ended in September 2005. Under these pilot programs, TSA collected biographical information and a biometric identifier from airline passengers who volunteered to submit to a security threat assessment, including a check of their identities against terrorist-related databases and appropriate criminal databases for outstanding warrants. For volunteers who passed the security threat assessment, TSA issued a credential, which uses the biometric information to verify identity when these individuals present themselves for screening at the airport security checkpoint. The enrollment population, which targeted frequent fliers obtained with the assistance of airlines, was capped at 10,000 volunteers. In 2005, TSA launched an additional pilot, the Private Sector Known Traveler Program, which involves partnering with the Greater Orlando Aviation Authority (GOAA). GOAA has contracted with a private sector vendor to collect information from participants and conduct marketing, operational, and customer service functions consistent with TSA guidelines. TSA's role focuses on conducting the initial security threat assessment and ongoing reassessments, as well as providing standards and oversight. This pilot is currently ongoing at Orlando.

Prior to the initiation of both pilots, TSA conducted a PIA to identify privacy related risks and administrative, procedural, and technical safeguards to mitigate these risks.[11] TSA continues to pursue the Registered Traveler Program, along with appropriate privacy considerations.

3. The Secure Flight Program

Secure Flight is a passenger screening program that implements the requirement, in Section 4012 of the Intelligence Reform and Terrorism Prevention Act, to move responsibility for the matching of airline

[11] Privacy Impact Assessments related to the Registered Traveler Program can be found in the Privacy Impact Assessment section of the Privacy Office website: www.dhs.gov/privacy.

passengers against the terrorist watch list from air carriers to the Federal government. During the period covered by this report, Secure Flight was in its initial test phase. TSA collected and analyzed historical passenger information to determine which data elements would provide the most robust watch list matching capability, while reducing the number of people misidentified through the screening process.

Prior to testing, TSA published the Secure Flight Test Privacy Package in the fall of 2004, which included a Notice of Proposed Rulemaking requesting data from the airlines, a SORN for the test records, and a PIA.

Congress instructed the Government Accountability Office (GAO) to review the program and certify that Secure Flight met the ten criteria listed in the enabling legislation, prior to TSA's launching the program. In June 2005, the GAO identified privacy concerns related to use of commercial data that TSA obtained during testing. These concerns were brought to the Privacy Office's attention. Although TSA updated and republished the PIA to provide more information on commercial data testing, the Privacy Office conducted an internal review of the privacy concerns raised by TSA's commercial data testing.

In brief, the Privacy Office review found that program personnel did not fully understand the privacy implications of its testing design; made material changes in its testing design over time, but did not update its initial public notices to reflect these changes; and collected commercial data on individuals to whom the program had not previously provided notice. A separate report on the review has been prepared by the Privacy Office.

In addition to providing general privacy guidance and specific advice on the required privacy documentation, the Privacy Office has strongly urged TSA to establish a more robust redress program and provided guidance on its planning for such a program. To date, TSA continues to work on developing its redress program in preparation for assuming responsibility from the airlines for passenger screening.

During the past ten months, the Privacy Office has partnered with the Secure Flight development team to provide privacy guidance throughout the continuing development of the program.

4. The Borders: US-VISIT

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program has a dedicated Privacy Officer who is accountable for compliance with applicable privacy framework and program requirements. During the time period covered by this report, US-VISIT added additional resources to its privacy team by filling a new Deputy Privacy Officer position, increasing contracted resources, and hiring a FOIA Officer.

US-VISIT embedded privacy principles in its systems and security architecture through the active participation of the privacy team in the program's development. The program conducted privacy risk assessments (PRAs) and PIAs that have been used to ensure that the program implements appropriate administrative, procedural, physical, and electronic safeguards to mitigate risk.

One example illustrating the building of privacy considerations into US-VISIT has been its implementation of the radio frequency identification (RFID) tags for monitoring entry into, and exit from, the U.S. US-VISIT, in conjunction with CBP, is testing the use of passive RFID tags to automatically, passively, and remotely record the entry and exit of covered individuals. These RFID tags are embedded in the Arrival-Departure form issued to international travelers (Forms I-94 and I-94W). The RFID tag will not contain, nor be derived from, any personal information. Instead, the RFID will contain a unique identification code, which will be linked at a port of entry with the biographic and biometric information collected when the traveler entered the United States. The Automated Identification Management System (AIDMS), which will match the RFID tag number with biographic and biometric information of the traveler, is a secure DHS computer system.

Implementation of the US-VISIT program is being conducted in increments, and the US-VISIT PIA is being updated as the increments are announced. Several PIA updates have taken place during the time period covered by this report. The PIA was updated on September 14, 2004, to include Visa Waiver Program (VWP) travelers covered under US-VISIT, the expansion of US-VISIT to the 50 busiest U.S. land border points of entry, and changes in the business processes used by DHS to share information with Federal law enforcement agencies. The PIA was updated again on June 15, 2005, to include the live test to read International Civil Aviation Organization (ICAO)-compliant, biometrically-enabled, travel documents by October 26, 2005. A third update of the PIA took place on July 1, 2005, including the implementation of technology (exit devices) and processes for recording the exit of covered individuals from air and sea ports by December 31, 2005.The proof of concept of this capability began in August 2005, and if successful, will be deployed to the 50 busiest land ports by December 31, 2007.

During this reporting period, the US-VISIT Privacy Officer instituted the Privacy Risk Assessment (PRA) process to conduct formal documented assessments of emerging US-VISIT policy issues concerning the program and technologies being investigated or implemented. Rather than reviewing all policy issues and technologies within a single assessment, the PRA provides distinct reviews that aid the developmental process for the program. US-VISIT conducts PRAs with the participation of key managers and staff involved directly with the particular policy issue or technology. Each PRA evaluates the privacy risk levels as low, medium, or high and details the mitigation strategies being or to be employed to keep the risks at the lowest appropriate risk level. Later, the Privacy Office and the US-VISIT Privacy Officer work to ensure that the program mitigates the identified risks to the proper risk level.

At the time of drafting the program's PIA, the program summarizes and includes all the analysis and results from the associated PRAs as well as the final decisions on the policy issues or technologies. This ensures that all developmental choices sustain and do not erode essential privacy protections.

A centralized and well-publicized redress process has been developed and implemented, providing individuals with a fast and easy way to review the personal information collected on them, have information corrected as appropriate, and if desired, appeal redress decisions to the DHS Chief Privacy Officer. In addition, informal agreements were reached with DHS components ICE, CBP, and USCIS, to process redress requests sent by mistake to US-VISIT and vice-versa.

Between its inception in January 2004 and June 2005, the US-VISIT program received approximately 80 redress requests. Similar figures hold for the past 12 months. US-VISIT has experienced a dramatic increase in redress requests from airlines due to outreach efforts made to inform them of the redress process. After a review, it was determined that the majority of the redress requests received from the airlines were not US-VISIT related and should be forwarded to CBP or returned if found to be a visa issuance complaint.

The US-VISIT Privacy Officer has a direct role in formulating policy relating to the application of privacy principles to the US-VISIT program. He developed and implemented requirements for privacy-compliant activities and operations, including the development of data usage agreements between US-VISIT and other agencies. US-VISIT updated its privacy policy in September 2004 to clarify how DHS shares information with Federal, state, local, tribal, and foreign law enforcement agencies.

C. Information Sharing and Other Interagency Work

Information sharing has become a significant focus of the Privacy Office during the reporting period. Several Executive Orders and Homeland Security Presidential Directives have been issued promoting information sharing, and the Privacy Office was actively involved in shaping these policy documents to include privacy protections.

In addition to Administration policy initiatives, a number of interagency working groups were established to deal with issues of interest to the Privacy Office. The office is an active participant in each of the interagency efforts described below.

1. Executive Orders and Homeland Security Directives

The Privacy Office led the effort, within DHS and across the Federal government, to build privacy protections into Executive Orders and Homeland Security Directives issued during the reporting period, and to develop a consistent privacy foundation across all Orders and Directives. The inclusion of the Privacy Office in the consultative process illustrates the Secretary's support for building privacy considerations into the design and implementation of homeland security programs as well as initiative at DHS and government-wide.

a) Executive Order 13356: Strengthening the Sharing of Terrorism Information to Protect Americans

Executive Order 13356 issued on August 27, 2004, directed all departments and agencies to enhance interchange of terrorism-related information within the Federal government and between the Federal government and appropriate authorities of states and local governments.[12] The Privacy Office was a leader in the effort to integrate privacy protections into the planning process supporting the implementation of Executive Order 13356, and in the larger issue of the design, implementation, and operation of an interoperable terrorism information sharing environment. The Privacy Office reinforced the importance of dedicated, in-house privacy officers and privacy training. The office further emphasized the need for initial privacy assessments and notifications, ongoing privacy audits and compliance reporting, and privacy officer-controlled centralized redress management.

b) Homeland Security Presidential Directive 11: Comprehensive Terrorist-Related Screening Procedures (HSPD-11)

HSPD-11 was issued on August 27, 2004, with the goal of implementing a coordinated and comprehensive approach to terrorist-related screening. The Privacy Office led the effort within DHS to integrate privacy protections at the earliest stages of HSPD-11 implementation. In both the strategic report and the implementation plan for HSPD-11, the Privacy Office reinforced the importance of a centralized redress process, in which the Chief Privacy Officer would have an active role, and the value of a permanent dedicated privacy officer, and privacy training for all staff involved in the screening process.

2. The Information Sharing Environment

The DHS Information Sharing and Collaboration Office (ISCO) was established to lead the creation of an Information Sharing Environment (ISE) within DHS and to assist with compliance with the requirements of recent Executive Orders and Homeland Security Directives. The Privacy Office provided a dedicated privacy staff member to ISCO for more than a year in order to ensure an understanding and integration of the application of Federal privacy frameworks to emerging information sharing initiatives and technical architectures involving multiple parties. These may include Federal, state, local, tribal, international, and private sector organizations.

To assist ISCO in its efforts, the Privacy Office developed guidance, detailing a rules-based description of the requirements that apply to information sharing under the Privacy Act. This guidance not only discusses how personal information may be shared, but also how the Privacy Act operates within the broader national and international legal and policy environment. This work, which included analysis of

[12] On October 25, 2005, Executive Order 13356 was revoked and replaced by Executive Order 13388 to further strengthen the sharing of terrorism information.

metadata planning into an information sharing architecture, was intended to aid the Department in creating a set of business rules for sharing personal information via the ISE.

The US-VISIT Privacy Officer has also worked extensively with the ISCO on an initiative to standardize all DHS data sharing initiatives and agreements. US-VISIT is the first DHS component to test and use the new format with internal and external data requesters.

A project directly related to the creation of the ISE, but managed by the DHS OCIO, is the effort to create a data reference model for the Department and the Federal government. Using metadata, the data reference model, which is part of the Federal Enterprise Architecture, will standardize the way in which DHS and the Federal government understands the data they collect and use.

Metadata is a classification technique that identifies the types of data available to a given system or a set of systems. Metadata holds great promise for privacy regulation, because in theory, all personal information could be identified and tagged, allowing for the creation of a set of rules that would apply to specific types of data in specific circumstances. With appropriate metadata and business rules in place, it would not be necessary to grant wholesale access to databases based on general grants of authority. Instead, access permissions could be tied to individual data elements and only the minimal amount of personally identifiable information would be exchanged. Furthermore, metadata could allow any use of personally identifying information to be tracked, further supporting privacy protections. The work being done by ISCO and the Policy Directorate on these issues, including standardizing data exchange rules, is expected to feed into the Data Reference Model project. The Privacy Office sits on the governing board of the Federal Enterprise Architecture initiative and is a member of the OCIO's Metadata Center of Excellence.

3. The President's Board on Safeguarding Americans' Civil Liberties

Executive Order 13353, issued August 27, 2004, created the President's Board on Safeguarding Americans' Civil Liberties to advise the President on "effective means" to "protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security homeland security functions."[13]

Several DHS personnel were appointed to the Board, including the Chief Privacy Officer. As one of the first orders of business, the Chief Privacy Officer conducted a survey of Federal agency practices regarding privacy and civil liberties. The results revealed that, while Privacy Act matters are addressed by every agency, privacy policy matters are not uniformly considered. Moreover, although most agencies have processes in place to deal with equal opportunity employment issues, Federal agencies do not address civil liberties issues in any systematic way. Based on the results of the survey, the executive director of the Board tasked the Chief Privacy Officer with developing privacy initiative recommendations from the Board that could be presented to the President. The Board was ultimately superseded in favor of the statutorily-created Privacy and Civil Liberties Oversight Board, which held its first meeting in March, 2006. The Executive Order Board's work influenced privacy policy initiatives, including OMB's effort to have senior officials for privacy and information policy named in all agencies. The Privacy Office has established a close working relationship with the new board and anticipates working with it on issues of mutual interest.

4. Leadership and Expertise in Interagency Working Groups

The Privacy Office participates in a variety of interagency activities. Some of these working groups are designed to permit information sharing between agencies on issues related to privacy and FOIA. In other cases, the Privacy Office brings privacy expertise to government-wide initiatives that involve new technology. Below are some examples of the Privacy Office's leadership role.

---

[13] A copy of Executive Order 13353, Executive Order Establishing the President's Board on Safeguarding Americans' Civil Liberties is at: www.whitehouse.gov/news/releases/2004/08/20040827-3.html.

a) The National Science and Technology Council's Subcommittee on Biometrics

The primary effort of the Privacy Office related to biometric technologies has been the role of its representative as the chair of the Social, Legal and Privacy Subgroup of the National Science and Technology Council's (NSTC) Subcommittee on Biometrics. The NSTC was established in 1993 by Executive Order 12881, as the principal means by which the President coordinates science and technology policy across the government and integrates the diverse parts of the Federal research and development enterprise.

The NSTC Subcommittee on Biometrics examines all issues related to the development and use of biometric technologies in the Federal government. Within this subcommittee, subgroups address specific biometric technologies, such as fingerprint and iris recognition. The Social, Legal and Privacy Subgroup is doing cross-cutting work relevant to all other subgroups. The Privacy Office leads the subgroup's work on the development of paper-based and online resources that can serve as a rich, centralized repository for information about the social history of biometrics, the legal framework that applies to collection and use of biometrics, and the privacy principles which should govern responsible use of biometric technologies.

b) The OMB Interagency Privacy Committee

The Privacy Office participates in the Interagency Privacy Committee chaired by OMB. This monthly forum allows privacy personnel from all Federal agencies to exchange views and information on issues of mutual concern. During this review year, the group has focused on developing guidance for HSPD-12, the executive directive calling for the issuance of a government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors. The Interagency Privacy Committee also provides a forum to discuss privacy best practices government-wide.

c) The FOIA Officers Homeland Security Information Group (FOHSIG)

The Director for Departmental Disclosure and FOIA and counsel to the Privacy Office represent the Department at quarterly meetings of the Justice Department's Office of Information and Privacy's (OIP) FOIA Officers Homeland Security Information Group, a working group convened by the Justice Department's Office of Information and Privacy, to discuss FOIA issues that affect homeland security. The group discusses pending litigation that could have a bearing on the government's ability to invoke FOIA exemptions to protect sensitive homeland security information, as well as procedural matters relating to homeland security.

D. The Data Privacy and Integrity Advisory Committee

In April 2004, DHS chartered the Data Privacy and Integrity Advisory Committee under the authority of the Federal Advisory Committee Act. The mission of the committee is to provide an external and expert perspective to advise the Secretary and the Chief Privacy Officer on DHS programmatic, policy, operational, and technological issues that affect privacy, data integrity, and data interoperability.

The twenty members of the committee were announced on February 23, 2005. The members of this committee have broad-based expertise in privacy, security, and emerging technologies.[14] Members come from large and small companies, academia, and the non-profit sector. The committee's charter calls for its members to serve four-year terms, although the initial cohort of appointees will serve staggered terms of two, three, or four years. All subsequent committee members will serve for a period of four years, as directed by the committee charter.

The Data Privacy and Integrity Advisory Committee organized itself into four subcommittees:

[14] A complete list of members and their affiliations can be found in the Privacy Advisory Committee section of the Privacy Office website: www.dhs.gov/privacy.

- **The Framework and Principles Subcommittee** considers the privacy questions and issues that the committee should address to ensure that DHS programs are reviewed consistently with fair criteria.
- **The Screening Subcommittee** reviews screening programs at the Department and provides appropriate recommendations for privacy protections and practices.
- **The Data Usage Policy Subcommittee** examines the Department's use of personal information and recommends policies on possible activities such as the use of private-sector data, data mining, and other data usage policies.
- **The Emerging Applications Subcommittee** examines the privacy implications of existing and new technologies and applications and ways to mitigate identified privacy risks.

Each subcommittee is chaired by a committee member and staffed by a member of the Privacy Office. The goals of the subcommittees are to work with the Department on developing objective analyses and memoranda on specific programs and policies; to educate the committee and the public; to provide recommendations to the full committee on the specific topics within their purview; and to help identify possible panelists and agenda items for committee meetings.

The committee holds quarterly public meetings to hear testimony regarding use of personal information by the Department and to hear from outside experts regarding the privacy issues affecting the Department. At the first meeting on April 6, 2005, in Washington, D.C., the committee heard from senior DHS policy makers, including Deputy Secretary Michael Jackson, who discussed their duties and responsibilities. The committee also elected its first chairman, Paul Rosenzweig of the Heritage Foundation, and vice chairman, Lisa Sotto of the law firm Hunton & Williams. The committee heard testimony from privacy experts and the public in the afternoon.

At its June 2005 meeting in Boston, Massachusetts, the committee reported on its new subcommittee structure and heard testimony on state-based perspectives on privacy and homeland security, the uses of screening by the Department, and new screening technologies and ways to mitigate privacy concerns related to the technologies. Appearing before the committee were: John Cohen, Homeland Security Policy Advisor for the Governor of Massachusetts; Acting Assistant Secretary Kenneth Kasprisin from TSA; Acting Commissioner Jayson P. Ahern from CBP; Justin Oberman, Assistant Administrator for Secure Flight and Registered Traveler from TSA; Patty Cogswell, Chief Strategist, US-VISIT; Donna Bucella of the Terrorist Screening Center; K. Krasnow Waterman of the DHS Information Sharing and Collaboration Office; Laura Manning of the DHS Homeland Security Operations Center; Norm Willox of LexisNexis; Daniel Weitzner of W3C; Dr. LaTanya Sweeny from Carnegie Mellon University; Dr. Simson Garfinkel from Massachusetts Institute of Technology; Jonathan Zittrain from Harvard Law School; Ari Schwartz of the Center for Democracy and Technology; Barry Steinhardt of the ACLU; and Annie Anton from North Carolina State University.

The committee held its September 2005 meeting in Bellingham, Washington. Here, the committee approved its first report, *Use of Commercial Data to Reduce False Positives in Screening Programs*, which presented the benefits and risks associated with commercial data use and discussed issues that DHS should examine when considering the use of commercial data in the screening context. The report contained several recommendations to govern the use of commercial data, including: collection minimization, strict access control, transparency, and application of Privacy Act restrictions.

In addition, the committee heard presentations on international perspectives on privacy and homeland security, the Secure Flight program, RFID technology at DHS, and risk-based analysis related to privacy. Participants included Trevor Shaw, Director General of the Audit and Review Branch of the Office of the Privacy Commissioner of Canada; Justin Oberman, Assistant Administrator at the DHS Transportation Security Administration; Michael Westray from DHS US-VISIT; Deirdre Mulligan of the University of

California-Berkley Law School; Lee Tien from the Electronic Frontier Foundation; and Peter Neumann of SRI Computer Science Laboratory.

The final meeting of 2005 was held in December in Washington, DC. The committee issued its second report, *Recommendations on Secure Flight*, which contained five recommendations, in brief, addressing the need for program transparency, a narrowly defined mission, data minimization, proactive redress, and holistic management.

The committee also heard presentations on the topics of security consistent with American freedoms and values, data analytics, redress at DHS, and cross-border cooperation. Participants included Paul Rosenzweig, then Acting Assistant Secretary for Policy and Counselor at DHS; Xuhui Shao of ID Analytics; Jeff Jonas of IBM; Mary DeRosa from the Center for Strategic and International Studies; Nancy Libin from the Center for Democracy and Technology; Virginia Skroski from TSA's Redress Office; Caroline Hunter of the Citizen and Immigration Services Ombudsman Office; Sandra Bell of Customs and Border Protection's Office of Regulations and Rulings; Jennifer Barrett of Acxiom; German Federal Data Protection Commissioner Peter Schaar; and Spanish Data Protection Authority representative Augustin Puente.

The committee began its second year in March 2006, hosting its quarterly meeting in Washington, D.C. Secretary Chertoff opened the meeting by thanking the committee for its efforts and advice, and discussed a range of privacy related topics in his remarks. Calling the DHS environment "probably one of the most challenging in government" with regard to addressing privacy concerns, the Secretary lauded the Privacy Office's work as "significant."

Secretary Chertoff also stressed privacy in his remarks, noting that because of the relative youth of DHS, there was " a lot of opportunity" to imbue the Department with "a respect for privacy" and a "thoughtful approach to privacy."

The committee adopted its third report, *Framework for Privacy Analysis of Programs, Technologies, and Applications*, which offers a framework for DHS to employ when considering the privacy impacts of "personal data-intensive programs and activities." The five steps of the framework are scope, legal basis, risk management, effects on privacy interests, and recommendations.

The committee heard presentations on topics such as a terrorism prevention study preview, building an information sharing environment, and operating within an information sharing environment. Participants included Betty Chemers and Herb Lin of the National Academy of Sciences; Dr. Carter Morris, Director, Information Sharing and Knowledge Management, DHS Intelligence and Analysis; Al Martinez-Fonts, Assistant Secretary, DHS Private Sector Office; Chet Lunner, Acting Director, DHS Office of State and Local Government Coordination; Jim Williams, Director, US-VISIT; Scott Charbo, DHS Chief Information Office; Luke McCormack, Chief Information Officer, U.S. Immigration and Customs Enforcement; and Frank DiFalco, Director, Homeland Security Operations Coordination.

The committee held its June 2006 quarterly meeting in San Francisco, California. The meeting featured its newly appointed chairman, J. Howard Beales, who is an associate professor of strategic management and public policy at George Washington University and former Director of the Bureau of Consumer Protection at the U.S. Federal Trade Commission. Lisa Sotto, a partner at Hunton & Williams, LLP, will continue to serve as vice-chairman. Both Beales and Sotto have served on the committee since its inception in April 2005, and will serve in their leadership positions through May 2007.

The committee heard presentations on topics such as state government perspectives on homeland security, border management and enforcement, closed-circuit television, US-VISIT and the advantages of using radio frequency identification technology in the immigration and border management enterprise, expectations of privacy in public spaces, and identity authentication.

Participants included Robert Saaman, Deputy Director for Federal Affairs, State of California Office Homeland Security; Charles DeMore of U.S. Immigration and Customs Enforcement; Clive Norris from Sheffield University Centre for Criminological Research, Sheffield, England; Steve Yonkers from US-VISIT; Nicole Wong of Google, Inc.; Deirdre Mulligan of the University of California at Berkley; Lillie Coney from the Electronic Privacy Information Center; George Valverde from the California Department of Motor Vehicles; Jim Dempsey of the Center for Democracy and Technology; and Jonathan Fox of Sun Microsystems, Inc. In addition, the committee hosted a public comment panel, which offered three members of the public in attendance the opportunity to address the committee on privacy issues of interest.

E. Government Transparency and the Freedom of Information Act (FOIA)

FOIA is a pillar of the U.S. privacy protection framework. A vibrant FOIA supports fundamental privacy principles of access, data integrity, and redress. This, in turn, leads to transparency of government operations, and transparency creates accountability.

As a relatively new agency of significant size and scope, DHS programs and policies have been and continue to be the subject of numerous Freedom of Information Act requests because of high public interest in its operations. For instance, in FY 2003 incoming FOIAs totaled 161,117; FY 2004 requests rose to 168,882; and in FY 2005 incoming requests numbered 163,016. Measures currently indicate that we expect an increased number of incoming requests for this fiscal year, as well.

The Department's FOIA Program, which is centralized for purposes of establishing policy, but managerially and operationally decentralized in each component, consists of 345 full time FOIA/PA processors and cost an estimated $28 million. Of the 208,717 requests available for processing in FY 2005, approximately 61% (126,126 requests) were processed to completion. The majority of FOIA/PA requests were from individuals and others (97.5%) with requests from media, commercial entities, and academia making up the remainder (2.5%) of FOIA processing activity. Only 0.7% of requests received a full denial. Of the 3,956 FOIA appeals available for processing, 22% (885 cases) were processed to completion. The majority of FOIA/PA appeals were made by individuals and others (94.3%) with the remainder (5.7%) of appeals made by media, commercial entities, and academia.

During the reporting period, the Department's FOIA group continued to work to merge the processes of multiple component agencies into a single program to support DHS as a whole. The majority of components actively participated in department-wide FOIA initiatives to define responsibility and accountability, manage workload, and support the policy coordination of the FOIA department-wide organization. The FOIA team provided guidance on determining which DHS components should have responsibility in cases where some files are shared between components, and on making final review from program offices before document releases. Continuing issues are the FOIA backlog and to better manage and address continuing increases in FOIAs to the largest components within the Department.

Executive Order 13392, Improving Agency Disclosure of Information, signed by President Bush on December 14, 2006, requires Executive Branch departments to reform their Freedom of Information Act programs in order to be more citizen-centered. The Executive Order contains several "deliverables." Departments must:

- Designate a Chief FOIA Officer at the Department level.
- Establish one or more FOIA Requester Service Centers to "serve as the first place that a FOIA requester can contact to seek information concerning the status of the person's FOIA request." To support the Service Center, the Chief FOIA Officer can designate FOIA Public Liaisons to whom a FOIA requester can raise concerns about service on FOIA requests.
- Review the department's FOIA operations, including the use of information technology, practices with respect to requests for expedited processing, implementation of multi-track processing, and

availability of public information through websites and other means. The review should also identify ways to eliminate or reduce the FOIA backlog.

- Develop a FOIA Improvement Plan that includes specific activities to eliminate or reduce the FOIA backlog, including changes to streamline FOIA processing and activities to increase public awareness. The FOIA Improvement Plan should have concrete milestones, specific timetables, achievable outcomes, and metrics to measure success.

- Submit a report to the Department of Justice (DOJ) detailing the Department's FOIA Improvement Plan and include updated Department performance information in its 2007 and 2008 annual FOIA reports to DOJ.

To prepare the preliminary report, each DHS FOIA Officer was given a template to summarize current FOIA operations. All reports provided an overview of the FOIA organizational structure within a DHS component or program, including budget and staffing figures, and information on FOIA operations. Much of the data requested is currently found in the DHS FOIA Fiscal Year 2005 annual report, posted on the Privacy Office and DHS FOIA website. FOIA Officers were asked to provide a processing overview, to include any field operations and administrative appeal functions. The remainder of the report then focused on an assessment of FOIA operations, including an assessment of current FOIA case backlog, aspects of case processing, such as implementation of multi-track processing, use of available FOIA-specific technology and expedited processing requests, availability of component-wide employee FOIA training, and utilization of the component's FOIA website. The DHS Acting Chief Privacy Officer/Chief FOIA Officer drafted an initial FOIA improvement plan from submissions of component FOIA operations across the Department, as required under Executive Order 13392.

In addition, the DHS FOIA Program implemented an improved, customer-friendly FOIA webpage and appointed FOIA Officers to additional DHS Headquarters' programs. These are just two examples of proactive strides taken by DHS FOIA in an effort to improve customer-service. On March 17, 2006, the Department established its primary FOIA Requester Service Center at the Headquarters level. To increase public awareness of FOIA, the Privacy Office also sponsored a public workshop on April 5, 2006, on *Transparency and Accountability: The Use of Personal Information within the Government*. A major focus of the program explored the U.S. Freedom of Information Act and its implementation, along with the special requirements of the Executive Order. The Privacy Office has been meeting regularly with representatives from the access community as well as immigration attorneys and advocates and will continue the discussion about FOIA matters.

Concurrent with policy and program development activities, the Privacy Office FOIA staff processed FOIA requests for programs of the Office of the Secretary, the Office of the Undersecretary for Management and its major program offices, and the Office of the Assistant Secretary for Policy, and its major program offices. Additionally, the Departmental Disclosure Officer served as a liaison to DHS Directorates and component agencies, forwarding to them FOIA and Privacy Act requests seeking records they maintain. The Privacy Office FOIA staff received 974 initial requests from August 1, 2005 through July 17, 2006. While over half of those requests were transferred to various DHS components, the remaining requests are processed by the Privacy Office FOIA staff. At the end of Fiscal Year 2005, the DHS FOIA Program had 355 requests pending. Due to the dedication of the DHS FOIA staff, the current pending caseload is below 50.

IV. RESPONDING TO NATIONAL AND GLOBAL CHALLENGES

Because the work of the Department is both national and international in scope, the work of the Privacy Office is equally broad. This section discusses Privacy Office activities that are not necessarily tied to any specific DHS program or component. Some of these activities involve national concerns that affect not only the work of the Department but also the broader perception of the appropriate interaction between the citizens and the government. Many of the activities described here are international in scope, and ones in which the Privacy Office represents the Department and the United States as part of the global community.

A. Examining Broad National Concerns

New data sources and new technologies can provide useful tools for the government's anti-terrorism efforts; however, they also raise concerns regarding individual privacy and civil liberties. The Privacy Office is an active participant in the national dialogue about appropriate uses of new technologies and about ways in which legal and policy frameworks can be adapted to meet the goals of national security and privacy protection.

1. Privacy Framework for Government Use of Commercial Data

Law enforcement has always had access to individuals' personal information, public records and various types of commercial data. Using subpoenas and other legal instruments, officers may have access to health, employment, financial, or transactional records.

The rise of the "information society" with its vast computer networks, inexpensive data storage, and sophisticated software has created new economic value in fast, inexpensive access to vast stores of information. To take advantage of this value, companies have arisen to aggregate and resell data about individuals to a variety of purchasers, for a variety of purposes. Commercially available personal information ranges from directory information, such as individual names, addresses, and telephone numbers, to records of retail purchases, including travel, insurance, and financial data, to public record information obtained from Federal, state, and local offices, including court documents, professional licenses, and property records.

The government's ability to access and analyze vast amounts of personally identifiable data collected by companies and data aggregators raises important privacy concerns. A number of reports have been issued urging that the government adopt standards for using such information for intelligence analysis, including the Department of Defense Technology and Privacy Advisory Committee (TAPAC) Report and reports by the Markle Foundation's Task Force on National Security in the Information Age.

The Privacy Office held a public workshop in September 2005 to inform the Privacy Office, DHS, and the public about the policy, legal, and technology issues surrounding the government's access and use of commercial information for counter-terrorism, and to explore how to protect individual privacy, given the government's need for better data analysis. The workshop provided a forum for considering standards for using commercially available data, as well as for examining whether and how information technology and commercial data can help improve national security while functionally protecting privacy. Finally, the workshop looked at technologies to aid in data analysis and information management that are more privacy protective.[15]

2. Appropriate Uses of Biometrics

A primary goal of the Privacy Office is to raise the level of privacy awareness of, and to develop active communications among, scientists and engineers who are investigating options and crafting

[15] Highlights and the full transcript of the workshop are available in the Privacy Workshop section of the Privacy Office website: www.dhs.gov/privacy.

proposals for DHS's technological responses to terrorism. The Privacy Office pursues this goal through active cooperation with scientific and technical organizations across DHS as well as with other government agencies, international organizations, and the private sector.

Biometrics, a measurable biological (anatomical and physiological) and behavioral characteristic that can be sued for automated recognition of individuals, is a technical area in which rapid development and deployment are taking place. Because of the highly personal nature of the information, the use of biometrics raises a number of privacy concerns ranging from concerns about the intrusiveness of the process by which biometric measurements are obtained, to the difficulty of "replacing" a biometric if a digital file containing biometric information is compromised, to the type of profiling and inferential tracking that might become possible as biometrics become pervasive.

The Privacy Office has been actively engaged, both within and outside the Department, in discussions about appropriate uses and protections of biometric information, particularly in the context of information sharing. In addition to its work on the DHS Biometric Coordination Group and chairing the Social, Legal and Privacy subgroup of the National Science and Technology Council's Subcommittee on Biometrics, the Privacy Office is also engaged in discussions on international biometric standards with various international organizations, including the International Organization for Standardization (ISO), ICAO, and the Organization for Economic Cooperation and Development (OECD).

In addition, in February 2004, the US-VISIT Privacy Officer was appointed chair of the U.S. component of the International Committee for Information Technology Standards (INCITS) Biometrics Working Group on Cross Jurisdictional and Societal Issues in the Implementation of Biometric Technologies. INCITS is a forum for the creation and maintenance of formal *de jure* information technology standards. INCITS is accredited by, and operates under, rules approved by the American National Standards Institute (ANSI). The US-VISIT Privacy Officer represents the U.S. government at international INCITS meetings.

In 2005, the Privacy Office participated in an international conference in Austria on privacy and biometrics. Privacy Office staff with international privacy and privacy technology expertise also participated in 2005 in the European Commission-sponsored conference on ethical and social implications of biometrics technology.

B. Data Mining

During the past year, the Privacy Office completed several reports relating to data mining issues. In response to complaints about DHS funding of an information sharing program that may have been lacking in privacy safeguards, the Privacy Office conducted a review of the *Multistate Anti-Terrorism Information Exchange (MATRIX) Program*. The program received a great deal of media attention and was considered very controversial, not only because it involved state governments' access to large amounts of personal information, but because of the public misconception that it involved the use of data mining techniques.

The Privacy Office's review found that MATRIX did not engage in data mining. It simply was a "proof of concept" project in which a private sector company's database technology was used by a coalition of states to enable their law enforcement investigators to access state-owned or publicly available records. The states' use of the information was solely for the purpose of pursuing investigative leads in support of specific criminal investigations. The pilot project was undermined and ultimately halted, however, largely because it did not provide transparency and privacy safeguards when it was first launched, causing the public to lose trust and the program eventually to lose state and Federal funding.

There is no set and agreed-upon definition of data mining. Definitions vary, with some stressing the discovery of relationships in large data sets, while others emphasize its goals as a predictive tool. These

differences in definitions also produce different opinions about the compatibility of data mining techniques with the preservation of privacy and civil liberties.

The Privacy Office recently sent to Congress a second report related to data mining. The Conference report on the Homeland Security Appropriations Act for Fiscal Year 2005 directed the Privacy Office to submit to Congress a report that examines data mining programs under development or in operation at DHS. As directed by Congress, the report provides a description of data mining technology, an assessment of the likely impact of the implementation of the technology on privacy and civil liberties, and a thorough discussion of policies, procedures, and guidelines that are to be developed to protect privacy and ensure civil liberties.

C. Working with the International Community

The Privacy Office also represents the Department in the international privacy community. The primary goal of the Privacy Office's international activities is to convey to the global community the importance of fair information practices to the office, the Department and the nation. Because information flows worldwide, in many instances regional initiatives and multilateral organizations are best positioned to develop and influence international privacy policy and practice. Bilateral relationships, on the other hand, play a role in addressing concerns with a particular country.

The Privacy Office, therefore, devotes significant resources to working with programs in multilateral global forums, such as OECD and the International Data Protection and Privacy Commissioners organization and on emerging privacy subcommittees within bodies such as ICAO and ISO. The Privacy Office also concentrates its work on issues with the EU, as well as within region-centric international organizations, including the Asian Pacific Economic Cooperation forum (APEC) and the International Working Group on Data Protection and Telecommunications (the Berlin Group). Additionally, the Privacy Office has addressed issues raised by the Joint Supervisory Body representatives of Europol and Eurojust. During the reporting period, the Privacy Office represented the U.S. government and DHS privacy policies at the following international forums:

1. The International Conference of Data Protection and Privacy Commissioners

The 26th annual International Data Protection and Privacy Commissioners Conference, which took place in Wroclaw, Poland, in September 2004, is the preeminent event for the global privacy community. The Conference brings together national data protection authorities from around the world and representatives of business, government and the public for a discussion of issues relevant to privacy and data protection. The last day of the conference is a closed session reserved for accredited representatives of government data protection authorities.

Participation in the Conference improves the U.S. government's ability to work with international partners on cross-border data sharing. It also provides a crucial opportunity to communicate with our global neighbors and the chance to dispel their perception that the U.S. interest in privacy protection and privacy rights is parochial and limited to protecting the privacy of Americans only.

The Wroclaw Conference represented a significant achievement for the U.S. government and the Privacy Office when the DHS Chief Privacy Officer was granted Observer status -- a first for any U.S. representative. The observer status, which allows admittance and participation in closed meetings of the conference, is a recognition and acknowledgment on the part of the international community of the leadership role played by the Privacy Office in shaping privacy policy within the U.S. government.

Substituting for the Chief Privacy Officer, Maureen Cooney, then Chief of Staff and Senior Advisor for International Privacy Policy, represented the Department and the United States at the Wroclaw Conference. She led off the Conference with a presentation addressing the Right to Privacy and the Protection of Public Security. Ms. Cooney emphasized that implicit in the title of the presentation is the

public expectation that the protection of both goals should be achievable and assured the international community that the Department shared that view. Moreover, Congress and the President mandated such protection in Section 222 of the Homeland Security Act, which requires that privacy policy and privacy compliance be integrated into the way in which DHS collects, uses, and shares personal information. Ms. Cooney noted that at DHS we understand that rhetoric, while important in promoting privacy awareness, is not enough – either to achieve privacy objectives in the government sphere or to engender trusted relationships with American citizens or visitors to our nation. Finally, Ms. Cooney emphasized the work ahead in facilitating a robust information sharing environment to combat terrorism, but one that should not over rely on technology or privacy awareness, but rather must incorporate the establishment of concrete safeguards and processes that prevent government from exceeding its proper bounds.

On September 14-16, 2005, the Privacy Office, together with a representative of the Federal Trade Commission, represented the United States at the 27th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Montreux, Switzerland. This was the third year of attendance for the U.S. delegation, which was attending at the invitation of the Swiss Federal Data Protection Commissioner, and the second year the Privacy Office was granted observer status in the closed session of data protection officials.

The Chief Privacy Officer delivered a presentation on building privacy protections into counter-terrorism structures. Ms. Kelly emphasized that the twin principles of transparency and accountability are the key to maintaining privacy in such systems. She started with the observation that, while the Privacy Office was organized differently than the European data protection model, it shared the common goal of ensuring privacy. Because the Privacy Office was well-placed inside the Department, it was able to ensure privacy protections were followed from the inception of any new information system. Ms. Kelly illustrated the point by discussing programs such as US-VISIT and the Computer Assisted Passenger Pre-Screening System (CAPPS II).

At its conclusion, the conference adopted a final declaration intended to strengthen the universal right of data protection principles ("Montreux Declaration"). The conference also adopted two resolutions, one on the use of biometric data in passports, ID cards, and travel documents; and the other on the use of personal data for political communication.

2. The OECD and the Enhanced International Travel Security Initiative (EITS)

The DHS S&T Directorate led an international initiative to build a conceptual model for secure international exchange of travel data through a distributed architecture. The EITS would concept would keep personal data within a traveler's nation of origin while also allowing destination nations to perform routine screening checks on travelers and travel documents.

The Privacy Office chaired the Privacy and Law Working Group of the EITS initiative. The Privacy Office provided informal guidance on the requirements for privacy protection to the S&T team and to the international and multi-agency project team. During the reporting period, the Privacy Office was actively involved in discussions with Australia and the United Kingdom about a potential pilot project to test a model of the EITS. The Privacy Office also holds a leadership role in presenting EITS for consideration before the OECD.

The Privacy Office is providing leadership on the appropriate use of biometrics and effective privacy notices for international travelers and for other purposes in connection with government programs. The office expects to continue its leadership role as the EITS concept is developed and tested further and as cross-border privacy enforcement mechanisms on a variety of travel issues continue to be explored.

3. ICAO: Privacy and Travel Documents

ICAO is a specialized body of the United Nations that sets standards for aviation safety, security, and efficiency, and encourages their implementation by the organization's 188 contracting states. As part of its mission, ICAO works on worldwide standards for international travel documents and the use of biometrics and PNR data. The Privacy Office is working with ICAO to shift the international privacy dialogue away from conflicting laws to compatible privacy principles in order to facilitate the appropriate sharing of PNR data and international travel documents, including biometrics.

4. Regional Initiatives

a) European Union (EU)

As described earlier in this report, the Privacy Office initiated a review of CBP's implementation of its Undertakings with respect to EU PNR. In tandem with this, the office also devoted considerable energy to organizing the Joint Review, including site visits, composition of the delegations, and related logistics. To support the DHS in larger cross-border cooperation efforts with the EU, the office provided a representative to the DHS team at the Policy Dialogue on Border and Transportation Security in Brussels, to assist in preparations for the Joint Review.

On September 20-21, 2005, delegations from DHS and the European Commission performed the first Joint Review of the Undertakings of CBP concerning PNR derived from flights between the U.S. and the EU.

The U.S. and EU review teams, led by Ms. Kelly and Francisco Fonseca Morillo, Director, Commission Directorate General Justice, Freedom and Security, engaged in two days of review and site visits. The teams comprised officials from border and transportation; data protection; and law enforcement, including representatives from EU Member States and senior CBP officials. The two teams were able to engage in a thorough set of questions and answers concerning U.S. privacy protection of the EU data. The discussions were candid and constructive.

The Privacy Office found that as of the date of the Joint Review, CBP was in full compliance with the terms of the Undertakings. CBP has put in place an extensive privacy program, which includes employee training and procedural and technical controls. Since the inception of the PNR program, the Privacy Office has received no reports of deliberate misuse of PNR information. A full copy of the report and Joint Statement of the parties can be found in the International Activities section of the Privacy Office website: www.dhs.gov/privacy.

In addition to travel related information sharing issues, the Privacy Office finds many issues of common concern that it listens and engages on with European privacy experts. Not least among these, the Privacy Office was the lead on Identity Theft discussions at the first European Data Protection Congress held in March 2006 in Madrid, Spain. Fraudulent use of lost and stolen passports and other travel and identity documents presents not only a terrorism threat to countries, but an identity theft threat to its citizens. The Privacy Office discussed these risks, along with the risks of insufficient data security of information systems, as a threat to critical infrastructures and to the integrity of personal information of individuals, leading to identity theft.

b) Asian Pacific Economic Cooperation (APEC)

The Privacy Office provided both counsel and leadership to a new APEC counter-terrorism initiative to detect lost and stolen passports, known as the Regional Movement Alert List (RMAL). The office reviewed the first ever memorandum of understanding with Australia on real-time sharing of information on lost and stolen passports to ensure that the data sharing arrangement properly protected privacy. As part of an effort to broaden the RMAL arrangement beyond Australia, the office served on a

U.S. government team to discuss expansion of RMAL, talking with counterparts from the U.K. and Australia.

In February 2005, Ms. Cooney chaired the U.S. Delegation's participation in an APEC meeting in Vietnam on implementation of the recently adopted APEC privacy principles. Ms. Cooney also presented at the APEC Symposium on Information Privacy in E-Government and E-Commerce. In the larger APEC context, the Privacy Office supports international dialogue that respects diversity of cultures, political, and economic backgrounds and promotes discussion of privacy protection based upon shared privacy principles and trusted implementation mechanisms, rather than focusing on conflicting laws as an impediment to privacy facilitated information sharing.

c) Other International Interests

In addition to dedicating a full-time Director of International Privacy Policy to oversee the review of all international privacy issues of the Department, the Privacy Office recently recruited additional staff with international experience in order to more comprehensively address privacy interests within North America with our partners in Canada and Mexico, as well as other regions of the world, including Latin America, Africa, and the Middle East.

Continuing international initiatives for the Department that the Privacy Office expects to provide counsel on include the Western Hemisphere Travel Initiative, to promote safe and efficient travel across U.S. borders with Mexico and Canada, and U.S. considerations of government to government cross-border information sharing protocols for anti-terrorism purposes that are privacy inclusive.

V. CHALLENGES AND OPPORTUNITIES FOR THE COMING YEAR

Looking forward, the major challenges for the Department and the Privacy Office will involve events that test the resolve across all parts of DHS to fully embrace the need to integrate privacy attentiveness, as well as data security and care, into the ways in which we routinely handle personal information as we carry out our security mission. At the same time, these challenges provide opportunities for the Department and the Privacy Office to take the lead in privacy awareness.

Additional challenges open the doors of opportunity, to advocates, to academics, to researchers, and, most of all, to the private sector, to help the Department meet its security mandate in ways that address the important privacy requirements of Section 222 of the Homeland Security Act and ensure the privacy right of individuals.

DHS has been given several statutory mandates to develop innovative border and immigration management control programs, to assist in the development of a driver's license or other state-issued document that can be relied upon for Federal purposes of verifying identity and to effectuate safe and efficient crossing along our northern and southern borders. Some or all of these initiatives may require technological assistance for information sharing and identity management to protect our citizens and visitors to the United States.

Finally, a continuing challenge for DHS is in developing and supporting a workable information sharing environment that will assist first responders, law enforcement, and the intelligence community in deterring and defeating terrorist activity. The opportunity to build vibrant privacy policies, access rules and controls, and audit features for use of shared and networked systems, that do not impede sharing, but that encourage responsible use by individuals with accountability, is an opportunity to be seized and, again, shared with public and private sector partners of the Department.

The Privacy Office is a ready partner in all of these challenges and opportunities.