Annual Report

Privacy Office Annual Report to Congress

July 2006 – July 2007

Homeland Security

Privacy Office
Annual Report to Congress
July 2006 – July 2007

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

July 2007

Letter from the Chief Privacy Officer

This is the third Annual Report issued by the Department of Homeland Security (DHS) Privacy Office. This report covers the period of July 2006 through July 2007. Annual Reports for 2003 to 2004 and 2004 to 2006 are posted on the DHS Privacy website at www.dhs.gov/privacy.

The Privacy Office has grown, not only in subject matter expertise, but also as an essential and supportive presence for the Department and its programs. During this reporting cycle, the Privacy Office made significant progress in its development of privacy resources and in outreach within the Department, as well as externally to other agencies, privacy advocates, and international data protection officials. The July 2006 to July 2007 Annual Report discusses the efforts of the Privacy Office over the past reporting year in compliance with the DHS Chief Privacy Officer's responsibilities as outlined in Section 222 of the Homeland Security Act of 2002, as amended.

As the DHS Chief Privacy Officer, I have worked to build upon the strong privacy foundation established by my predecessor. My focus as the Chief Privacy Officer has been to formalize the processes and operations of the Privacy Office to ensure that it can fulfill its statutory requirements and be a true partner within the Department to support the important mission of the agency.

We continue to make progress in our outreach to DHS components and programs to increase compliance with privacy documentation – Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and Privacy Act System of Records Notices (SORNs) for programs and systems involving personally identifiable information (PII). Compliance efforts included updating and disseminating our popular DHS *Privacy Impact Assessment Guidance* for 2007 and conducting tutorial workshops to train Federal employees and contractors on the development and use of PIAs.

In response to growing Federal attention to privacy issues, DHS has been a leader in issuing guidance responsive to these issues. The Privacy Office developed guidance documents regarding the use of Social Security numbers (SSNs), protections afforded to non-U.S. persons, and a privacy incident handling response plan for the Department. Additionally, the Privacy Office has implemented an inventory process aimed at reducing the use of SSNs within the Department.

We are working closely with our colleagues in the Department to ensure that privacy protections are integrated into DHS programs and rulemakings. Through our efforts to increase the transparency of high-profile Department initiatives, we have participated in rulemakings, contributed to PIA and SORN development, and actively sought to address privacy concerns raised by Congress, the privacy community, and the public. In addition, the Privacy Office

continues to work with our international partners, expanding both our international outreach and DHS and Federal involvement in international privacy initiatives.

Looking ahead, we see our next Annual Reporting cycle as a period of significant opportunity for the Department to expand the presence of Privacy Officers and Privacy Points of Contact (PPOCs) within DHS operational components. Our Disclosure and Freedom of Information practice will continue it efforts to substantially reduce Freedom of Information Act (FOIA) request backlogs in components and to improve the efficiency of the Department's FOIA process.

Thank you for supporting the Privacy Office and its mission. I look forward to working with you as we continue to infuse DHS with a culture of privacy.

Hugo Teufel III
Chief Privacy Officer

U.S. Department of Homeland Security

Table of Contents

1. Overview of Privacy Activities (Executive Summary)

The strategic goals of the Privacy Office include the responsibilities set forth in Section 222 of the Homeland Security Act of 2002 [Public Law 107-296; 6 U.S.C. 552], as amended. The DHS Chief Privacy Officer's responsibilities include:

> (1) Assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information;
>
> (2) Assuring that personal information contained in Privacy Act systems of records is maintained in full compliance with fair information practices as set out in the Privacy Act of 1974 [5 U.S.C. § 552a];
>
> (3) Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
>
> (4) Conducting privacy impact assessments (PIAs) of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;
>
> (5) Coordinating with the Office for Civil Rights and Civil Liberties (DHS CRCL) to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner, and that Congress receives appropriate reports on such programs, policies, and procedures; and
>
> (6) Preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.[1]

The Privacy Office is structured into two functional units: Privacy and Departmental Disclosure and FOIA. The Privacy unit manages and formulates the above statutory and policy-based responsibilities, in a collaborative environment with each component and program, to ensure that all privacy issues are provided the appropriate level of review and expertise. The Departmental Disclosure and FOIA unit assures consistent and appropriate Department-wide statutory compliance with the Freedom of Information Act of 1966, as amended [5 U.S.C. § 552], and requests made under the Privacy Act.

The Privacy Office has other general statutory and policy-based responsibilities, including implementation of Section 208 of the E-Government Act of 2002 [Public Law 107-347] and serving as the primary point of contact for DHS for the development of privacy policy involving the implementation of the Information Sharing Environment (ISE) as set forth in Guideline 5 of Executive Order 13388.

---

[1] The authorities and responsibilities of the Chief Privacy Officer are further amended by the Implementing the Recommendations of the 9/11 Commission Act of 2007 [Public Law 110-53], passed on August 3, 2007. The Privacy Office's implementation of the Chief Privacy Officer's responsibilities, as amended, will be reported in the next Annual Report.

The Privacy Office fulfills its responsibilities under the Privacy Act and the FOIA by integrating the implementation of the Privacy Act's fair information principles into every aspect of privacy management at DHS. The fair information principles include the principles of Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. DHS uses the fair information principles to enhance privacy protections by assessing the nature and purpose of all PII collected to fulfill DHS's mission to preserve, protect, and secure the homeland. DHS's implementation of the fair information principles is described below:

- The Principle of Transparency is implemented through the publishing of PIAs, SORNs, and Privacy Act Statements (also known as "(e)(3) statements," referring to its Privacy Act citation);
- The Principle of Individual Participation is implemented through DHS's commitment and legal requirement to provide individuals with means of accessing their PII. This principle is implemented by providing the public and individuals notice of access and redress programs through the publishing of PIAs, SORNs, and Privacy Act Statements. DHS implements this principle through DHS redress processes and through DHS's Privacy Act and FOIA programs;
- The Principle of Purpose Specification is implemented by ensuring that the purpose of a program is specified throughout the development of the underlying system, and this is then documented as part of PIAs, SORNs, and Privacy Act Statements, as applicable;
- The Principle of Minimization of PII is considered a critical part of the development of the underlying system and must be documented within PIAs, SORNs, and Privacy Act Statements, as applicable;
- The Principle of Use Limitation is implemented through the PIA, where the program documents why a program needs particular data elements, and through the SORN, where the program describes the purposes for the collection and the type of data sharing anticipated. These notices must be completed prior to the system becoming operational;
- The Principle of Data Quality and Integrity requires that programs have written, published standard operating procedures outlining how to review information for compliance with the relevant data quality and integrity standards. These procedures should be documented in the PIA and SORN. In addition, programs must develop and implement records retention schedules in compliance with the National Archives and Records Administration (NARA) guidelines;
- The Principle of Security is implemented through the Certification and Accreditation (C&A) process outlined by the Federal Information Security Management Act of 2002 (FISMA) [Public Law 107-347] and is overseen by the DHS Chief Information Security Officer (CISO); and
- The Principle of Audit and Accountability is implemented throughout the lifecycle of a program. During the development of the program, the program

must identify the needs for certain audit capabilities and training requirements. These will be captured in the C&A and the PIA. Also, on a daily basis, personnel must be vigilant in their handling of PII to ensure that the information is not subject to loss, unauthorized access, destruction, use, modification, or unauthorized disclosure.

Through its efforts, the DHS Privacy Office has sought to apply the fair information principles to the full breadth and diversity of the information and interactions of DHS.

2. Activities of the Department

The overarching mission of the Privacy Office is to build a culture of privacy across the Department. Any DHS program that involves the collection and use of PII receives the attention of the Privacy Office. Building privacy into DHS programs leads to informed and standardized information management practices. In order to protect privacy, programs must understand what information is collected and the reason for the collection, as well as how the information flows both internally and externally. The Privacy Office assists program managers, system owners, and decision-makers in addressing privacy throughout the system's lifecycle. Programs should conduct a PTA, PIA, and Privacy Act SORN at the beginning of project planning. Conducting privacy analyses early in the development process results in better information management, better information security, and ultimately, helps the program to garner support from the public, the advocacy community, and from Congress and the Office of Management and Budget (OMB).

2.1. Compliance

Operational responsibilities for the Privacy Compliance group include supervising the completion and approval of all PTAs, PIAs, and SORNs throughout DHS. Additionally, the Privacy Compliance group conducts privacy reviews of DHS programs, as appropriate.

As part of the compliance process, the Privacy Compliance group works with a number of existing DHS-wide programs to ensure that privacy is integrated into the Department. In particular, the group reviews all OMB Exhibit 300 budget submissions to determine whether new and existing programs have appropriately addressed privacy. During the Fiscal Year (FY) 2008 budget process, the Privacy Compliance group denied approval of four investments because of insufficient privacy protections and privacy documentations. The Privacy Compliance group is now closely coordinating with the four affected programs to embed privacy into the developmental and operational processes to provide appropriate protective measures.

A critical goal for the Privacy Compliance group over the next year will involve updating and revising operational components' SORNs to reflect information oversight and integration within DHS. The U.S. Coast Guard (USCG) and the U.S. Citizenship and Immigration Services (USCIS) will be the first components to completely update their legacy agency-era SORNs.

2.1.1. Privacy Threshold Analyses

Although PIAs are commonly preformed throughout the Federal Government, the DHS Privacy Office developed the PTA in November 2005 as part of the C&A process for assessing the security of information technology (IT) systems. The PTA was specifically designed to identify which systems in the DHS information system inventory collect or use PII, which systems require a PIA, and which need a SORN. The Privacy Office has further refined the PTA over the past two years and it is now a key aspect of the privacy compliance process.

The PTA outlines general information about a system, including the year the system was developed, description of the system, and what PII the system collects or uses, if any. After the Privacy Compliance group reviews the PTA, a detailed dialogue with the program manager, information security officer, or PPOC, as necessary is implemented. The Director of Privacy Compliance determines whether a full PIA or SORN is needed based on these precedents. If the PTA analysis demonstrates that a full PIA is required, the program must complete the PIA using the DHS *Privacy Impact Assessment Guidance* and return the completed document to the Privacy Office for review and approval.

The Privacy Compliance group uses the PTA not only to officially document the privacy requirements of IT systems in the DHS inventory undergoing C&A, but also to formally document other decisions made by a program affecting privacy. For example, a program may seek to access the DHS Global Address list, which contains DHS employee contact information (including DHS e-mail address, work telephone number, office location, etc.), in order to conduct a survey of the workforce for human resource analysis. This program must complete a PTA documenting how the data will be used, how data will be accessed, and how or when the data will be shared. The PTA formally documents the parameters for the survey, providing specific documentation of how the survey may affect the privacy of DHS employees. As another example, DHS has published a DHS-wide PIA covering contact lists. When a program considers itself a candidate to fall under this DHS-wide PIA, the program completes a PTA certifying that it meets the appropriate requirements for the PIA. The PTA formally documents that the program meets the requirements, and then the program is allowed to proceed with its collection of contact data with the knowledge that its operations are appropriately documented by a published PIA.

A template for the PTA is available on the Privacy Office website, www.dhs.gov/privacy, under the "Privacy Impact Assessment" webpage. From July 2006 through July 2007, the Privacy Office reviewed and validated approximately seven hundred and eighty-two (782) PTAs.

2.1.2. Privacy Impact Assessments

PIAs are a key aspect of the Department's privacy compliance efforts. By conducting PIAs, DHS demonstrates its commitment and consideration of privacy during the development of programs and systems, thus upholding the Department's commitment to maintaining public trust and accountability. By documenting the procedures and measures through which the Department protects the privacy of individuals, the Department can better carry out its mission.

Section 208 of the E-Government Act requires all Federal agencies to conduct and complete PIAs for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222(1) of the Homeland Security Act, as amended, requires the Chief Privacy Officer to ensure that the technology used by the Department sustains and does not erode privacy protections. The Chief Privacy Officer is also required by Section 222(4), as amended, to conduct PIAs for proposed rulemakings of the Department. The PIA is a crucial mechanism used by the Chief Privacy Officer to fulfill his statutory mandate.

Based upon the experiences of the past year, the Privacy Office issued a 2007 update to its *Privacy Impact Assessment Guidance, 2006,* reflecting the requirements of both Section 208 of the E-Government Act and Section 222(4) of the Homeland Security Act, as amended. This update helped to clarify and improve upon the questions asked. The Privacy Office first published PIA guidance in July 2005 and updated it in May 2006 and May 2007. The guidance provides detailed instructions for conducting and completing a PIA, and is posted on the Privacy Office website, www.dhs.gov/privacy. The PIA Guidance with the PIA template has been used, adapted, and adopted by numerous other Federal agencies.

PIAs demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire system development lifecycle. A PIA provides an analysis of how PII is collected, stored, protected, shared, and managed. For example, in January 2007, USCIS issued a PIA on its Integrated Digitization Document Management Program (IDDMP), which is a new IT system that digitizes the paper-based Alien Files (A-Files) into a new electronic format. In addition, PIAs have provided greater transparency into Customs and Border Protection (CBP)'s implementation of the air phase and the land/sea phase of the Western Hemisphere Travel Initiative (WHTI).

The Privacy Office coordinates the completion of PIAs for the Department and the components. The Chief Privacy Officer approves all Department and component PIAs. PIAs and summary abstracts are posted on the Privacy Office website at www.dhs.gov/privacy, and a compendium of posted abstracts is published in the *Federal Register* (FR) on a monthly basis.

Between July 2006 and July 2007, fifty-four (54) PIAs were approved and published. The Privacy Office also reviewed and approved two (2) PIAs for National Security Systems for Intelligence and Analysis. Given the sensitivity of the systems, the PIAs will not be published. A synopsis of all approved PIAs is provided in the Appendix.

2.1.3. PIA Guidance

As privacy compliance at DHS has matured, so has the content and procedures for conducting a PIA. The lessons learned from previous reviews have translated into better content for each upcoming PIA. In May 2007, the Privacy Office issued an update to its popular *Privacy Impact Assessment Guidance, 2006.*[2] The updated guidance, *Privacy*

[2] The 2007 PIA Guidance does not require programs to update existing Departmental PIAs. The Privacy Office is accepting all PIAs submitted using the former template as programs transition to the updated guidance and template.

Impact Assessment Guidance, 2007, reflects the progress and outreach of the DHS Privacy Compliance group as the PIA process continues to evolve and mature.

It is important to note that the updates to the PIA Guidance document, while not numerous, are a direct reflection of requests for greater clarity in certain sections of the guidance in response to comments from DHS components. While some questions were re-written to more accurately capture information, other questions were consolidated to reduce redundancy. Most importantly, the Privacy Office expanded the discussion section of those questions to clarify their purpose.

To summarize the major changes:

- The introduction for PIA Guidance added new discussion points aimed at capturing a system's typical transaction or data flow. The development and completion of a PIA benefits greatly from a full description of each step of the system's information handling, from collection to storage to sharing and destruction.
- Section Two underwent two changes. First, the question directed at data mining was edited to expand the potential scope of the question and clarify any confusion over the term "data mining." Second, a question was added on the use of commercial data.
- Section Three was modified by consolidating three questions; Sections Four, Five, and Eight had several questions consolidated into one to reduce redundancy.
- Section Nine added new questions, replacing the existing ones to reflect decision points in the system development lifecycle. This change enables system owners, program managers, and privacy officers to see the consistency between the narrative of the PIA and the development of a system or program.

Each of the described changes directly affects the quality of the privacy analysis in the PIA. Significant attention was and continues to be given to the PIA discussion of how privacy risks are mitigated. As noted above, these changes are not a wholesale change of former practices; rather, they represent refinements to better capture a program or system's information practices and associated privacy issues.

The Privacy Office will continue to work with the component and headquarters program managers and system owners to further refine the PIA template as needed.

2.1.4. Reviewing and Updating Systems of Records Notices

Section 222(2) of the Homeland Security Act, as amended, authorizes the Chief Privacy Officer to "assure that personal information contained in Privacy Act systems of records is handled in full compliance with fair information principles set out in the Privacy Act." Compliance with the Privacy Act requires that each Department component maintaining PII in a "system of records,"[3] provide notice of such system – implementing the fair

[3] 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)].

information principle of notice. Every Federal agency provides notice by publishing SORNs in the *Federal Register*. The Privacy Office guides and assists component programs with the drafting and issuance of SORNs for all new collections and uses of PII and for all significant changes to an existing system of records. DHS has many legacy systems of records that remain operative in accordance with the notice provided by the legacy agency and the savings clause [Section 1512] of the Homeland Security Act. Nonetheless, the Privacy Office is reviewing existing systems of records maintained by each of the DHS components and will publish updated SORNs in the *Federal Register*. To achieve this goal, the Privacy Office is assisting the components to update existing SORNs and to integrate all departmental record systems, eliminate duplicative systems, and ensure a consistent PII policy across the Department.

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 PII. The Privacy Office provides DHS components with standardized guidance on drafting SORNs and generic language for routine uses to incorporate, as necessary, into each notice. These notices are then drafted by the program office and forwarded for review and clearance to the Privacy Office, with final review for legal compliance with *Federal Register* standards by the Office of the General Counsel (OGC). For example, USCIS issued an updated SORN for its Verification and Information System (VIS), originally published under the Justice/INS-035 SORN on October 17, 2002 [67 FR 64134]. The VIS SORN provides notice to the public on form I-9, *Employee Eligibility Verification*, which is the basis for employers to verify the eligibility of individuals for employment through VIS.

Since 2006, the Department has published seventeen (17) new or revised SORNs. A synopsis of all new or revised SORNs is provided in the Appendix.

2.1.5. OMB Exhibit 300s

A central feature of the Privacy Office's Privacy Compliance operation is the OMB Exhibit 300 IT investment review process. Also referred to as the "OMB 300" process, the Privacy Office's review is both substantive and procedural, ensuring that each investment has the proper privacy documentation in place at the correct time. Specifically, the review of each system includes an examination of the privacy protections implemented within the system, and whether the protections are documented in a PIA or SORN. The Privacy Office evaluates and scores each investment based on its responses to a standardized set of questions, and ensures that the appropriate documentation has been completed. The Privacy Compliance group then works with each investment program manager to complete necessary documents. The Privacy Office works in close cooperation with the DHS Chief Information Officer (CIO) and the DHS Chief Financial Officer (CFO) to ensure that DHS IT investments meet the established legal and policy standards set forth by DHS, OMB, and Congress.

During the FY 2008 budget process, the Privacy Compliance group recommended for approval over one hundred (100) investments that included the appropriate privacy documentation. Conversely, the Privacy Office rejected four investments because of insufficient privacy protections and privacy documentation. The Privacy Compliance group has worked with each of the four programs to ensure that the appropriate

protections and privacy documentation are in place. As of July 2007, two rejected investments have subsequently been revised and recommended for approval by the Privacy Office and DHS to OMB.

2.1.5.1. FISMA Certification and Accreditation

FISMA establishes a comprehensive framework for ensuring the effectiveness of the Federal Government's IT program. FISMA also establishes a framework of information security controls over Federal information resources. As part of FISMA compliance, each Federal agency must document that an IT system meets technical and security standards through the C&A process.

The Privacy Office works closely with the DHS CISO to ensure that DHS IT systems with PII have met the appropriate privacy requirements within the C&A process. As part of its compliance reporting requirements to OMB, the DHS C&A process requires a formal notification that either a PIA is required or the determination that no PIA is necessary. The Privacy Office reviews the privacy documentation, PTA, PIA, and SORN, for each system undergoing C&A review. At a minimum, each system is required to submit a PTA. As noted above, the PTA outlines general information about a system, including the year the system was developed, a description of the system, and what personal information the system collects or uses, if any. After the Privacy Compliance group reviews the proposed investment and converses with the program managers, information security officer, or component privacy officer, the Director of Privacy Compliance determines the required privacy documentation and whether additional documentation is required.

If no PIA is necessary, the completed and approved PTA is sufficient as privacy documentation, and the system may move forward, having satisfied the privacy elements of the C&A process. If a PIA is necessary, the system owner or component privacy officer is responsible for drafting the PIA and working with the Privacy Compliance group to complete the PIA and SORN (if necessary). These close working relationships assist program managers and system owners and contribute to their understanding of the Privacy Office as a resource that they can leverage to meet DHS regulatory requirements.

The C&A process is important to the Privacy Office's Privacy Compliance operation because it allows the Office to monitor new and developing systems and to develop and maintain close working relationships with the DHS CIO, DHS CISO, program managers, system owners, and information security officers across the Department. The Privacy Office works closely with the DHS CIO and values its relationship with the information policy and information security offices in the Department.

Based on feedback from the program and system owners as well as from Department senior leadership, the Privacy Office will continue to further refine the use of PTAs, PIAs, and SORNs in the C&A process to ensure that privacy issues are adequately identified and addressed in the beginning of the information system's lifecycle.

2.1.5.2. DHS Investment Review Process

The Privacy Office works in close partnership with the DHS CFO and the DHS CIO to review major Departmental investment projects for each fiscal year. The Privacy Office

serves as the privacy subject matter expert in this important review process. In addition, the Privacy Office is a member of the Department's Integrated Program Review Team (IPRT), which is part of the Investment Review process for the Department. The process of determining and executing the necessary privacy documentation serves as a beginning point with many programs during the development and execution of the investment review process.

In connection with the investment review process, the Privacy Office is also a member of the Enterprise Architecture Center of Excellence (EACOE), which provides input to the Enterprise Architecture (EA) Board. Through this process, the Privacy Office works with programs to integrate the Privacy PTA, PIA and SORN processes into the development lifecycles of the IT programs of the Department.

2.2. Privacy Office Coordination with Component Privacy Offices

2.2.1. Component Privacy Officers and Privacy Points of Contact

Establishing and increasing the number of well-trained privacy officers at the component level helps to ensure that privacy is built into new and existing programs at the beginning of the development process. Component privacy officers and PPOCs ensure that programs in their component agencies identify privacy issues and work with the Privacy Office to address them. Currently, the Transportation Security Agency (TSA) and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program have full-time privacy officers. Several components have PPOCs, who work on a daily basis with the DHS Privacy Office.

The designation of privacy officers within each operational component is a high priority for the Privacy Office. While the Privacy Office retains expertise in all types of privacy issues, the overall mission of the Privacy Office is increasingly demanding. The component privacy officers will report to the component head, but will coordinate with the Privacy Office for privacy compliance and Department-wide initiatives. The long-term goal of the Privacy Office is for each component to prepare all privacy documentation (PTAs, PIAs, and SORNs) at the program or system development level, provide the first stage review at the component privacy level, and then have the Privacy Office conduct the final review to approve the privacy documentation. The component privacy officers will also be responsible for managing other privacy compliance programs as mandated by the DHS Privacy Office.

The Privacy Office works closely with component and program privacy officers, and PPOCs to implement privacy across the Department. TSA and US-VISIT have privacy teams comprised of full-time staff led by privacy officers, dedicated to supporting privacy processes within the components. CBP, USCIS, and the Federal Emergency Management Agency (FEMA) have PPOCs who handle component privacy-related matters, including the processing of programs and systems through the privacy compliance operation, assisting with drafting PTAs, PIAs, and SORNs, and responding to unauthorized disclosure incidents involving PII.

Increasing the number of component privacy officers and PPOCs would support better privacy implementation throughout the development and implementation lifecycle of a

program. Additional component privacy officers and PPOCs will allow the Privacy Office to focus on Department-wide policy development, coordination of privacy processes from a Departmental view, and the establishment of standard, uniform, and repeatable processes for privacy.

2.2.2. Privacy Protection Initiatives with Component Privacy Offices

DHS component privacy officers and PPOCs are responsible for ensuring that components and programs maintain a culture where privacy is valued and fundamental to how business is conducted within the component or program. This section discusses privacy activities in several high-profile DHS organizations: TSA, the US-VISIT program, and CBP.

2.2.2.1. Transportation Security Administration

The TSA Privacy Officer is responsible for developing privacy policies and TSA compliance with applicable privacy authorities 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, has developed a series of policies and procedures within TSA to enhance trust in TSA and to ensure the protection of citizens and the traveling public. During the past year, TSA has taken steps to augment its professional privacy staff and was the driving force behind a variety of data protection initiatives. Below are some highlights of the TSA Privacy Officer's regulatory and policy activities during this reporting period.

2.2.2.1.1. Screening Transportation Workers

TSA published a joint Final Rule with USCG to implement a Transportation Worker Identification Credential (TWIC) program to provide a biometric credential used to confirm the identity of workers in the national transportation system. As a result of this rulemaking, TSA will conduct security threat assessments on each individual before issuing the credential. The TSA Privacy Officer prepared an updated PIA that reflects changes made to the TWIC program in response to public comment on the Notice of Proposed Rulemaking (NPRM) and lessons learned from the TWIC Prototype program. As designed and proposed in the NPRM, TWIC can be used in conjunction with access control readers designed to recognize the credential and the information encrypted on it, to permit authorized individuals to enter secure areas of port facilities and vessels without escort. While the Final Rule does not require the installation of card readers at this time, the expectation is that TWIC will be used with access control systems in the future. TSA has designed the credential and verification process to maintain strict privacy controls so as to prevent a TWIC holder's biographic and biometric information from being compromised.

The TSA Privacy Officer participated in the development of the NPRM and continues to work to incorporate privacy principles into TSA's systems and security architecture, and into its program-based PIAs.

2.2.2.1.2. Airline Passengers and Registered Traveler

2.2.2.1.2.1. Secure Flight

Secure Flight is a passenger screening program, established by Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) [Public Law 108-458], that envisions shifting more responsibility for matching of airline passengers against the terrorist watch list from air carriers to the Federal Government.

TSA continues to progress towards the launch of the Secure Flight program. During the period covered by this report, Secure Flight has submitted a Secure Flight NPRM, SORN, and Privacy Act Exemption NPRM to OMB and drafted a new PIA to reflect the updated proposed implementation of the Secure Flight program. Working in concert with the Acting Privacy Officer for Secure Flight, the TSA Privacy Officer, and the DHS Privacy Office, the Secure Flight development privacy team identified risks and appropriate mitigation strategies and has made substantial progress toward ensuring that the program will continue to operate within the structure of currently published notices during its ongoing development.

TSA initiated a comprehensive review of the Secure Flight program in response to risks identified by the Government Accountability Office (GAO) and the Privacy Office's report on its review of Secure Flight. The TSA review resulted in a "re-baselined" program with a focus on security and privacy in the foundations of the Secure Flight program. In evaluating new requirements for the Secure Flight program, TSA analyzed 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 and minimizing the data necessary to conduct watch list matching.

In addition to providing general privacy guidance and specific advice on the required privacy documentation, the TSA Privacy Officer and the DHS Privacy Office have assisted in establishing a more robust TSA redress program in anticipation of assuming responsibility from the airlines for passenger screening.

Finally, both the TSA Privacy Officer and the DHS Privacy Office have collaborated with the Secure Flight privacy development team to enhance outreach efforts to privacy advocates and other Federal, State, or local aviation industry stakeholders. As part of their outreach, the Secure Flight program plans to seek comments from industry stakeholders, privacy advocacy groups, and the public through a NPRM before finalizing the regulation.

2.2.2.1.2.2. Testing Screening Technologies

TSA is testing various technologies designed to enhance security at security screening checkpoints. One of the technologies being tested is X-ray "backscatter" technology.

Backscatter is a voluntary option for passengers undergoing secondary screening as an alternative to the physical pat-down procedures currently conducted by Transportation Security Officers (TSOs) at a security screening checkpoint. Backscatter technology utilizes a stand-alone screening station that allows TSOs to detect non-metallic devices

and objects, as well as weapons or other harmful objects that a passenger may be carrying on his or her person. The TSA Privacy Officer has worked closely with the vendors and TSA executive leadership to build individual privacy protections into the technology. For example, the backscatter scanning system does not allow the TSO to print, store, or transmit an image of an anomaly; each screening station is a stand-alone machine (rather than a network) that is located remotely from the general screening area. TSA is currently testing backscatter systems and other technologies at the Phoenix Sky Harbor Airport and will expand testing to the John F. Kennedy International Airport (JFK) and the Los Angeles International Airport (LAX). These tests will provide an operational evaluation that will assist in determining expansion opportunities.

Another technology being tested for security screening purposes is passive millimeter wave technology. This technology detects and measures millimeter waves naturally emitted by the human body to screen individuals for anomalies that could be explosives. The TSO views a video image of the passenger and the monitor indicates whether an object blocking the waves may warrant secondary screening.

Passive millimeter wave technology was tested at Washington D.C.'s Union Station in July 2007 to determine the effectiveness of procedures for screening individual passengers for concealed explosives in the rail environment. The technology passively screened passengers as they passed through a doorway, allowing as many passengers as possible to be screened on a random basis, and did not impact passengers and did not delay trains. Signs were posted in boarding areas to give individuals advance notice of the screening. No PII was collected during this testing. The video images are not saved. TSA also tested this technology in the commuter ferry environment aboard New York's Staten Island Ferry in April 2007.

2.2.2.2. US-VISIT

The US-VISIT program has a dedicated privacy officer who is responsible for compliance with applicable privacy laws, regulations, and US-VISIT privacy requirements. The program's privacy officer is also responsible for creating and sustaining a culture within the US-VISIT program office where privacy is highly valued and fully integrated into the business operations and Enterprise Life Cycle Methodology (ELCM). Under the US-VISIT privacy officer's direction, US-VISIT has built a strong internal privacy program based on policy, principles, and rules of behavior, and a training and awareness program.

2.2.2.2.1. Protection of Traveler Privacy through Privacy Compliance

A primary goal of US-VISIT is to protect the privacy of visitors to the United States. Compliance with this goal is important to maintaining the credibility of US-VISIT in foreign travelers' eyes. As part of meeting this goal, US-VISIT has been the department leader in implementing DHS Privacy Policy Guidance Memorandum 2007-01, *Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*. Under this policy, US-VISIT handles all non-U.S. person PII held in mixed systems in accordance with the fair information principles, as set forth in the Privacy Act. In addition, US-VISIT was one of the first programs to provide foreign travelers with an

opportunity for redress, thereby allowing them to inquire about their records and have them corrected, if necessary.

Developments in the US-VISIT program are evaluated and reflected in PIAs, SORNs, and updates to other relevant program privacy documentation. The PIA for the initial deployment of the US-VISIT program was the first PIA to be conducted at DHS. US-VISIT PIAs and SORNs continue to be regularly updated as new US-VISIT projects are implemented. Examples of PIAs for these projects include:

- On March 27, 2007, the PIA for the Arrival and Departure Information System (ADIS) was updated to: (1) clarify that I-94 data from land ports-of-entry is also used by and stored in ADIS, in addition to CBP's Treasury Enforcement Communications System (TECS); and (2) notify the public of the inclusion and use of Form I-94 data in ADIS to include air, land, and sea ports-of-entry.
- On May 14, 2007, the PIA for the Automated Identification Management System (AIDMS) was updated to evaluate the proof of concept for technology and processes for automatically recording the entry and exit of covered individuals at U.S. land border ports-of-entry using Radio Frequency Identification (RFID)-enabled I-94 Arrival/Departure Forms. Both the AIDMS PIA and SORN were revised to reflect the decommissioning of the RFID Proof of Concept. All data previously stored in AIDMS will be deleted or destroyed.
- On May 25, 2007, the PIA for the Automated Biometric Identification System (IDENT)[4] was updated to describe changes to IDENT required to support enumeration, a new service provided by IDENT. Through enumeration, DHS assigns a unique personal identifier, known as an enumerator, to each individual for whom DHS has collected biometrics (i.e., ten fingerprints) and a minimal set of biographic information. The enumerator will be used to link and retrieve disparate immigration and border management records, allowing for linkage and retrievably with a single identifier instead of multiple identifiers. This project is being developed in coordination with USCIS for use in their Adoption Pilot.
- In July 2006, the IDENT PIA and SORN were updated in conjunction to reflect a new routine use of the information so that the public has notice that biometric and limited biographic information can be processed for intelligence in addition to the existing uses (such as for national security, law enforcement, immigration, intelligence and other DHS mission-related purposes).
- On September 1, 2006, a PIA was produced for the Interim Data Sharing Model (iDSM) for the IDENT/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability project. As anticipated under the External Data Sharing section of the IDENT PIA, this document discusses the sharing of data between IDENT and the Department of Justice (DOJ)/FBI Criminal Justice Information

[4] IDENT is the primary repository of biometric information held by DHS in connection with its several and varied missions and functions, including but not limited to: the enforcement of civil and criminal laws (including immigration laws); investigations, inquiries, and proceedings in connection with those missions and functions; and national security and intelligence activities.

Service (CJIS) Division's IAFIS. FBI/CJIS provides criminal history information to Federal, State, and local law enforcement agencies. The FBI completed its own PIA on the data it shares with IDENT. Therefore, the US-VISIT PIA focuses only on the DHS sharing of IDENT data with the FBI/CJIS.

Since its inception in 2003, US-VISIT has published a total of thirteen (13) public privacy notices, including PIAs and PIA updates, as well as two SORNs. As the US-VISIT program provides its identity management services to additional entities, these PIAs and SORNs will continue to be updated and published, giving the public advance notice and continued insight into the program.

2.2.2.2.2. US-VISIT Outreach and Coordination

US-VISIT conducts coordination and outreach with external partners to build a culture of privacy capable of supporting the US-VISIT mission. For example, the US-VISIT Privacy Officer reviews all external data sharing requests not currently covered under existing agreements, and takes the lead on conducting privacy risk assessments and drafting any resulting data sharing agreements. These data sharing agreements, often formalized in Memoranda of Understanding (MOUs), contain explicit privacy and security requirements to govern access to, and disclosure and retention of, PII. From July 2006 to July 2007, the US-VISIT Privacy Officer has taken a leadership role for developing MOUs on US-VISIT's behalf, including an MOU that provided the USCG with mobile identity-verification capabilities for the first time.

Furthermore, the US-VISIT Privacy Officer engages internal and external audiences to create a quality dialogue on privacy. Within US-VISIT, the US-VISIT Privacy Officer enlists guidance and expertise from the Mission Operations and IT branches to securely deliver PII in support of mission operations. Within DHS, US-VISIT has turned to the DHS Privacy Office for guidance on privacy compliance, and privacy documentation review and approval. Outside of the governmental enterprise, US-VISIT program has received recommendations on best practices for risk mitigation and privacy enhancements from privacy advocacy groups such as the American Civil Liberties Union (ACLU), the Electronic Privacy Information Center (EPIC), and the Center for Democracy and Technology (CDT).

2.2.2.2.3. Responding to Requests for Redress

The US-VISIT redress process system, first established during the 2003-2004 implementation of the US-VISIT program, has been transitioned to support the DHS Traveler Redress Inquiry Program (TRIP) system for receipt and processing. The vast majority of these inquiries received by US-VISIT have centered on requests for information about the program, requests for personal records, or requests for access to or correction of records outside the purview of US-VISIT. Between July 2006 and July 2007, US-VISIT received two hundred and thirty-two (232) inquiries, resulting in a total of more than nine hundred (900) inquiries since the program's inception.

The results of these inquiries can be broken down into three types of responses:

- Forty-two (42) US-VISIT redress requests (of one hundred and eighty-five (185) total) have been received, handled, and a response issued to the requestor.

- Ninety-four (94) issues that were not within US-VISIT's purview (of three hundred and ninety-nine (399) total) have been received and forwarded to the appropriate agency, and a notification issued to the requestor.
- Ninety-six (96) requests for personal records (FOIA) or general information (of three hundred and twenty-three (323) total) have been received and a response issued to the requestor.

2.2.2.3. Customs and Border Protection

CBP has a PPOC who acts as the liaison between the DHS Privacy Office, the CBP Office of Information Technology (CBP OIT) and CBP programs. In addition, the CBP PPOC and his staff are responsible for addressing privacy issues related to information sharing that CBP conducts with Federal, State, and local agencies, including the development of MOUs for information sharing.

CBP PIAs and SORNs are regularly updated as new projects are implemented. Examples of PIAs for these programs include:

- On July 14, 2006, CBP issued a PIA for the modernization of the Automated Commercial Environment (ACE) and International Trade Data System (ITDS). The purposes of ACE are to streamline business processes, to facilitate growth in trade, to ensure cargo security, to provide means to combat terrorism through monitoring what materials and which persons enter and leave the country, and to foster participation in global commerce, while ensuring compliance with U.S. laws and regulations. To that end, ITDS builds upon the existing infrastructure of ACE in sharing electronic international trade and transportation data with participating Federal agencies.
- On November 1, 2006, CBP issued an updated PIA for the Global Enrollment System (GES) to describe its new online application process for enrollment in CBP trusted traveler programs. The CBP PPOC and the Privacy Office coordinated on the development of this PIA.
- On November 22, 2006, CBP issued a PIA for the Automated Targeting System (ATS). ATS is an enforcement screening tool consisting of six separate components, all of which rely substantially on information in the Treasury Enforcement Communications System (TECS). ATS was covered under the SORN for TECS historically. As detailed below, CBP took the additional step of issuing a separate SORN for ATS, even though the types of information collected and the purpose of the collection had not changed. This SORN did not describe any new collection of information and was intended solely to provide increased notice and transparency to the public about ATS. The ATS SORN was published on November 2, 2006.
- On January 23, 2007, CBP issued the PIA for the air phase of the Western Hemisphere Travel Initiative (WHTI).
- On July 20, 2007, CBP issued the PIA for Project 28 of the Secure Border Initiative-net (SBI-net), the initial demonstration of technological

enhancements to assist CBP officers and Border Patrol Agents in hardening and securing the land border environment. The PIA covers the camera and communications technology used to monitor the border, and persons crossing the border, during the initial test phase. SBI-net is the technological application of the President's Secure Border Initiative, a multi-year effort to strengthen security and control of the U.S. land border.

2.2.2.3.1. Automated Targeting System

On November 2, 2006, CBP issued a Privacy Act SORN for ATS [71 FR 64543]. DHS received a number of comments and extended the comment period until December 29, 2006[5]. A total of six hundred and forty-one (641) comments were received in response to the SORN. Historically, the SORN for TECS covered ATS.[6] As part of DHS's updating of its SORNs, and in an effort to provide more detailed information to the traveling public and trade community, DHS provided notice of ATS as a separate Privacy Act system of records, giving greater visibility into ATS targeting and screening efforts.

ATS is a decision-support tool that compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. ATS allows DHS officers charged with enforcing U.S. law and preventing terrorism and other crime to effectively and efficiently manage information collected when travelers or goods seek to enter, exit, or transit through the United States.

In response to the comments, the Privacy Office assisted CBP in updating the ATS SORN and PIA. These updated documents are available on the Privacy Office website, www.dhs.gov/privacy.

2.3. DHS Credentialing Programs

To conduct trusted data transactions, a government agency needs to know with whom it is dealing. The Federal Government is therefore working to establish processes that establish trusted credentials to link an asserted identity with a physical person. However, the process of collecting information to verify someone's identity can raise significant privacy issues, such as what information is collected, how it is managed, and who has access to the information. Furthermore, agencies must have a clear process in place to verify government credentials without compromising the privacy of the individual. During this reporting period, the Privacy Office has been involved in multiple initiatives to ensure that privacy is integrated into agency identity-proofing programs and initiatives.

---

[5] Notice of the comment period extension was published in the *Federal Register* dated December 8, 2006 [71 FR 71182]

[6] The publication by DHS of a SORN and PIA for ATS does not change the scope of the collection of information by ATS-P and the functionally possessed in the screening and targeting capabilities of ATS previous covered by the SORN for TECS.

2.3.1. REAL ID

As part of its statutory responsibilities, the Privacy Office is responsible for conducting PIAs 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 [Public Law 109-13].

The REAL ID Act sets forth minimum issuance standards for State-issued drivers' licenses and IDs. 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 (DOT) and State governments, 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 purposes of 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 Privacy Office participated in drafting and reviewing the NPRM issued on March 9, 2007 [72 FR 10819]. In addition, the Privacy Office funded a contract in 2006 to explore the creation of a State federation to implement the information sharing among the States 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.

In response to the NPRM, the public filed thousands of comments, most of which raised privacy concerns about the REAL ID Act and the proposed regulations. The Privacy Office is working with the DHS rulemaking team to address the comments and to issue the final rule. In addition, the DHS Privacy Office has conducted a PIA of the NPRM. The PIA is posted on the DHS Privacy Office website at www.dhs.gov/privacy. The PIA will be updated as necessary when the rule is final.

2.3.2. Western Hemisphere Travel Initiative

The IRTPA requires DHS and the Department of State (DOS) to develop and implement a plan to require all travelers, U.S. citizens, and foreign nationals to present a passport or other acceptable document that denotes identity and citizenship when entering the United States. WHTI is the joint DOS and DHS plan to implement this recommendation of the National Commission on Terrorist Attacks upon the United States (the 9/11 Commission) and the Congressional mandate. The purpose of WHTI is to strengthen border security and facilitate entry into the United States for U.S. citizens and legitimate international visitors.

Generally, individuals applying for admission to the United States from foreign points-of-departure are required to show a valid passport or passport and visa. The exception has been U.S. and Canadian citizens entering the U.S. across the land borders, who have not been required to either carry or present identity and citizenship documents. Given new security concerns, this exception makes it difficult to conduct appropriate security screening. An Advanced Notice of Public Rulemaking (ANPRM) for the land/sea phase of WHTI was published in the *Federal Register* on September 1, 2005, and a final rule

for the air phase of WHTI that was published in the *Federal Register* on November 24, 2006. WHTI requirements were implemented for air travel on January 23, 2007.

On June 26, 2007, DHS published a NPRM in the *Federal Register* [72 FR 35087] on the proposed implementation of the land/sea phase requirements for WHTI. DHS and DOS are engaged in a rulemaking process to implement the land/sea phase of WHTI. The proposed rules will require most U.S. citizens entering the United States by sea or land ports-of-entry to have either a U.S. passport; a U.S. passport card; a trusted traveler card such as NEXUS, FAST, or SENTRI; a valid Merchant Mariner Document (MMD) when traveling in conjunction with official maritime business; or a valid U.S. military identification card when traveling on official orders. The NPRM also outlines ongoing efforts to provide other alternative documents.

The Privacy Office provided privacy guidance during the rulemaking process. A key privacy issue has been the DHS proposal to use facilitative technology on this passcard, such as vicinity RFID. The Privacy Office has been closely involved in DHS discussions regarding WHTI and with the development of the land/sea NPRM. The Privacy Office issued the PIA for the air phase of WHTI which is posted on the Privacy Office website at www.dhs.gov/privacy. The Privacy Office updated this PIA to reflect the WHTI requirements set out in the final rule for the air phase. The Privacy Office is working to issue the PIA for the land/sea NPRM.

2.3.3. Traveler Redress Inquiry Program

DHS created TRIP to serve as a single destination for individuals who have inquiries or seek resolution regarding difficulties they have experienced during their travel screening at transportation hubs – such as airports and train stations – or crossing U.S. borders. DHS TRIP is a gateway that integrates individual DHS component redress programs, such as TSA's Traveler Identity Verification Program (TIVP) and US-VISIT's redress program discussed above.

DHS TRIP serves several DHS components, including TSA, CBP, USCIS, U.S. Immigration and Customs Enforcement (ICE), US-VISIT, DHS CRCL, and the Privacy Office. DHS TRIP facilitates communication of redress results across DHS components so that travelers cleared for one program can be cleared for other DHS programs.

DHS TRIP must collect PII from the individual requesting redress in order to resolve the underlying issue, which often involves misidentification of an individual. Individuals may file a Traveler Inquiry Form, which allows individuals to detail their experiences, such as:

- Watch list misidentification issues;
- Situations where travelers believe they have faced screening problems at ports-of-entry; or
- Situations where travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at U.S. transportation hubs.

As of July 1, 2007, DHS TRIP has received approximately eleven thousand seven hundred (11,700) redress requests.

The Privacy Office was involved in the development of DHS TRIP, working with the DHS Screening Coordination Office, DHS CRCL, TSA, USCIS, and CBP to ensure that information provided by the public through DHS TRIP was protected consistent with the provisions of the Privacy Act. In addition, the Privacy Office worked with TSA to ensure that a PIA and SORN for DHS TRIP was in place and publicly available on the Privacy Office website, www.dhs.gov/privacy.

2.3.4. Homeland Security Presidential Directive 12

Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004), requires the development and promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. HSPD-12 specifies secure and reliable identification that:

- Is issued based on sound criteria for verifying an individual employee's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Is issued only by providers whose reliability has been established by an official accreditation process.

Through its implementation of HSPD-12, DHS is working to identify and reduce inconsistent agency approaches to facility security and computer security that are inefficient and costly, and increase risks to the Department.

The Privacy Office worked with the OMB Personal Identity Verification (PIV) Privacy Working Group to develop the sample privacy documentation, including the templates for the PIA and two SORNs. The Privacy Office also reviewed and approved the PIA and the SORNs. The first SORN covered the management of the PIV system and the second SORN covered the retention of background investigatory material.

The Privacy Office is currently working with the DHS Office of Security on the Final Rule regarding the exemptions from certain Privacy Act requirements for the background investigation SORNs and to examine and analyze DHS's implementation of the PIV system in connection with HSPD-12.

3. Technology

The first responsibility of the DHS Chief Privacy Officer listed in Section 222 of the Homeland Security Act, as amended, is to assure that the use of technologies sustains privacy protections relating to the use, collection, and disclosure of personal information. The Chief Privacy Officer fulfills this responsibility by implementing fair information principles in the Department's technology programs and initiatives, evaluating and integrating privacy protections into privacy-sensitive technologies, and providing privacy expertise directly to the Office of the Chief Information Officer (OCIO) and the DHS Directorate for Science and Technology (S&T).

3.1. Radio Frequency Identification

The Privacy Office continued its participation in the DHS RFID Working Group (RFIDWG), and sought to integrate privacy protections into the strategic and management documents coordinated issued by the group. The Privacy Office collaborated with the RFIDWG to draft its charter, which makes meeting privacy protection standards one of its primary responsibilities. In addition, the Privacy Office contributed substantial input during the development the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-98 *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, which, while primarily focused on security, presents both substantive and procedural guidance regarding privacy compliance requirements that apply to the use of RFID technologies.

3.2. Biometrics

The Privacy Office continued its leadership role with the National Science and Technology Council's Subcommittee on Biometrics and Identity Management. In this capacity, the Privacy Office assists the members of this inter-agency effort in addressing privacy issues raised by the research and use of biometrics, both biometric information and technology, across the Federal Government. Ongoing projects with the Subcommittee include:

- Developing high-level, long-term strategies for integrating privacy protection into the use of biometrics across all levels of government;
- Advising on privacy impacts of various information sharing models related to biometrics; and
- Working with the International Privacy Policy group to develop guidance regarding international privacy policy frameworks that would apply to biometrics.

In addition, the Privacy Office continues its participation in DHS's Biometrics Coordination group and provided ongoing advice to DHS components on privacy issues, including issues related to the role of PII in biometric templates.

As part of its outreach efforts, the Privacy Office spoke on privacy at biometric events organized by the Defense Science Board Task Force on Defense Biometrics and at the 2006 Biometric Consortium Conference.

3.3. Enterprise Architecture

The DHS Enterprise Architecture (EA) empowers DHS to capitalize on advances in technology and standardization across the entire Department. As mentioned above, the Privacy Office works in close partnership with the Office of the CFO and the OCIO to review major Departmental IT investments for each fiscal year. These investment reviews enable the Department to ensure that proposed IT initiatives align with the overall technology architecture of the Department, and that as much as possible, existing assets are reused and new capabilities are added systematically and with a view toward standardization. The Privacy Office reviews proposed IT investments to ensure that

proposals that appear to use PII comply with DHS privacy protection requirements. This year, the Privacy Office reviewed thirty-five (35) proposed IT investments.

In addition to IT investment reviews, the Privacy Office also worked with the OCIO Data Management Working Group (DMWG) to build privacy protections into the mechanisms DHS uses to manage data across the department. The Privacy Office integrated privacy protection principles into the DHS data management policy tenets and is currently working with the DMWG to integrate privacy compliance requirements into the overall data reference model to be used as an inventory tool and a process to improve the methods of data reuse and information sharing across DHS. This effort will build privacy protections into that process, so that as new systems identify existing PII that the Department already maintains, those systems also address the privacy compliance requirements that are triggered by the use of PII.

Also, the Privacy Office is currently working with OCIO to build privacy protection procedures directly into the new DHS system development life cycle that will govern how all IT systems are developed across the Department. Once finalized, the new system development life cycle will articulate the specific privacy compliance requirements that should be addressed as part of each stage of the development lifecycle.

3.4. Service Oriented Architecture

Part of the Department's EA is the implementation of Service Oriented Architecture (SOA). SOA enables IT developers to build individual modules of discrete functionality that can be reused across multiple systems and even across multiple organizations. SOA enables the rapid development of agile IT solutions by integrating pre-existing modules instead of building individual stand-alone systems.

This new architecture provides more efficient use of staff and system resources, as well as more effective control, uniform and updated system processing, cost savings, and it facilitates greater information sharing and interoperability.

SOA also presents new challenges. As the development environment becomes more flexible and as data becomes more accessible to reuse, the required analysis and protections of how PII is used and controlled becomes more complex. To this end, the Privacy Office worked closely with the OCIO at both the headquarters and component levels to ensure that privacy protections are integrated into the EA, the SOA and its component parts.

The Privacy Office worked with the OCIO Methods and Standards Focus Group to develop a set of security and privacy standards and methodologies for the development and operation of the Enterprise Service Bus (ESB), which is the infrastructure that supports services across the Department. The Privacy Office followed this work with additional collaboration with the OCIO SOA Tactical Focus Group's development of a SOA framework and the additional work of the DHS SOA Services Lifecycle Tiger Team.

The Privacy Office also worked with USCIS to develop a PIA for both a component level ESB and an individual service. Both PIAs are available on the Privacy Office's website

at www.dhs.gov/privacy. These PIAs will serve as models for an enterprise level PIA for all future ESBs to ensure consistent and comprehensive privacy protections.

4. Privacy Complaints

4.1. Privacy Complaints

Pursuant to Section 222(6) of the Homeland Security Act, as amended, the DHS Chief Privacy Officer is required to report to Congress on the Department's resolution of complaints involving privacy violations. The Privacy Office receives complaints and inquires from the privacy community and also responds to Congressional oversight regarding privacy matters at the Department. The Office also receives communications from the general public in various formats.

4.1.1. Addressing Complaints from the Privacy Community and Responding to Congressional Oversight

The Privacy Office meets regularly with members of the privacy community to provide information about the Privacy Office's activities and to learn what questions or concerns they may have about the Privacy Office or the Department. During these outreach meetings, the privacy community has expressed its concerns regarding the Department's screening programs, such as ATS, Secure Flight, and US-VISIT; rulemakings, such as REAL ID and WHTI; and the use of technologies, such as RFID and video surveillance. In addition, the privacy community has expressed concerns about Passenger Name Recognition (PNR) negotiations and data mining programs. Congressional oversight requests were related to similar issues.

During this reporting period, the Privacy Office released two reports on data mining in response to Congressional oversight requests. In July 2006, the Privacy Office released the *Data Mining Report: DHS Privacy Office Response to House Report 108-774.* This first report was completed pursuant to House Report 108-774: *Making Appropriations for the Department of Homeland Security for the Fiscal Year ending September 30, 2005, and for Other Purposes*. In June 2007, the Privacy Office completed work on its second report on data mining in response to House Report 109-699 – *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes,* which was released in early July 2007.

As a result of the increasing focus on data mining issues, the Privacy Office sought to educate components about the privacy issues related to data mining activities. The Privacy Office is also exploring establishing a coordination group to review data mining standards and synchronize the development of guidance across the Department.

The Privacy Office also addressed concerns raised by the privacy community regarding potential privacy violations. In July 2006, the ACLU requested that the Privacy Office initiate an investigation into allegations that Federal Air Marshals (FAMs) were required to meet a monthly quota for filing Surveillance Detection Reports (SDR). The ALCU noted that several news reports, both printed and televised, identified situations where FAM field supervisors were suspected of directing FAMs to file a specific number of SDRs per month. The Privacy Office, in conjunction with the TSA Privacy Officer,

investigated the situation and determined that no such quota existed, in either formal policy or as a de facto requirement. In response to the ACLU request and subsequent Privacy Office inquiry, FAM field management clarified TSA policy requiring accurate and credible SDRs as outlined in an August 2004 memorandum. In addition, the TSA Privacy Officer investigated the ACLU's claim that individuals may be added to a watch list as a result of an SDR; the Privacy Office determined that not a single individual had been added to a watch list as a result of a SDR. The ACLU complaint and the Privacy Office response are available on the Privacy Office website, www.dhs.gov/privacy.

In addition to its reports to Congress, the Privacy Office undertakes reviews in response to public concerns, including requests by the privacy community. The Privacy Office issued its reviews of the Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project and the Secure Flight Program in December 2006 and July 2007, respectively, and issued its review of the DHS S&T Directorate's ADVISE program in July 2007 in response to concerns raised by the privacy community.

4.1.2. Internal Processes that the Privacy Office Uses to Respond to Privacy Concerns

As mentioned above, the SORN process provides transparency into DHS programs and information collections subject to the Privacy Act. DHS receives public comment on high-profile SORNs, such as the ATS SORN, when they are published in the *Federal Register*. The Privacy Office works with the overseeing component to review the comments and to develop an appropriate response.

The Privacy Office also responds to complaints regarding internal matters that affect privacy. For example, in July 2006, a union representative for the American Federation of Government Employees (AFGE) contacted the Chief Privacy Officer regarding the unauthorized distribution of PII by a USCIS service center. The incident involved the distribution of spreadsheets listing USCIS detail volunteers that was forwarded to the listed detailees and their supervisors. The spreadsheets included the names, position title, and duty location for each of the detailees, as well as their SSNs. AFGE filed a grievance with USCIS, requesting notification of all affect personnel that their information was disclosed and requesting that USCIS take steps to ensure that the spreadsheets were destroyed. In addition, the AFGE requested that USCIS provide additional training for agency personnel on Privacy Act protections. USCIS responded to this incident and has fully complied with the AFGE's remediation recommendations.

Additionally, Section 8305(4) of IRTPA requires the Privacy Office to work with the DHS CRCL to coordinate and communicate on matters that overlap both offices. The Privacy Office and CRCL have worked together on DHS TRIP, REAL ID, DHS Fusion Centers, and several international initiatives.

4.2. Handling Questions and Comments from the General Public

- ~ *How do I file a Privacy Act/Freedom of Information Act request?*
- ~ *Who is responsible for overseeing the "No Fly" watch list?*

~ *I think this proposed program will impact my rights as a taxpayer of this country…*

The DHS Privacy Office receives many inquiries, comments, and complaints from members of the public. These questions come to the Privacy Office through telephone calls, e-mails, written letters, and faxes. Many of these questions come from individuals seeking information regarding issues beyond the scope of DHS and/or the Privacy Office, such as questions regarding the USA PATRIOT ACT, passports, and drivers' licenses. Other individuals have sought to make DHS aware of suspected illegal aliens living in their communities. Privacy Office staff members respond to these inquires, and, if necessary, direct the individual to the appropriate component for a response. The Privacy Office provides an e-mail address through the Privacy Office website, privacy@dhs.gov, which members of the public use to contact the office.

During this reporting period, the Privacy Office received approximately four hundred (400) e-mails, representing comments, inquiries, and complaints. The Privacy Office primarily receives requests for information about filing Privacy Act requests or requests for copies of training presentations or guidance documents. In response, the Privacy Office has expanded the number of documents available through the Privacy Office website, www.dhs.gov/privacy to proactively respond to many of these requests.

However, the majority of outside communication that the Privacy office receives involves issues outside of the Office's purview. When these comments, complaints, or requests are received, the requests are referred to the appropriate DHS component or other Federal agency. Examples of issues raised by such e-mails include:

- **CAPS II** – An individual asked, "Why should DHS invest in programs (e.g., CAPS II) that rely upon inaccurate information? Can DHS guarantee that there is a process to correct a CAPS II file so that innocent people can get their names off of the no-fly list?"
- **Traveler Experience** – An individual submitted this comment regard the NPRM for Secure Flight [TSA-2004-19160], "Our horror story can not be told in 2000 characters. Is there somewhere I can e-mail or fax the whole nightmare story?"
- **Customs and Immigration Concerns –** An individual inquired, "My children, who are Canadian citizens, recently visited the United States. Neither during their departure from Milwaukee nor when checking in for their connecting international flight were they asked to hand over form I-94W. I am contacting DHS to request assistance. Please tell me what is necessary to document my children's departure from the United States to avoid any problems when they re-entering the United States in the future."
- **Screening Watch Lists** – An individual notes, "While flying to Hawaii in 2005, my husband and I discovered that we were placed on a watch list. We submitted Traveler Identity Verification forms and requested to be removed from the watch list. While my husband has received an acknowledgement of the receipt of his request, I am still waiting for a response. I have left numerous messages on the TSA phone system but no one is returning my calls."

- **Immigration Status** – An individual writes, "I am requesting DHS assistance in resolving a "name check" being performed by the FBI as part of my immigration application. An application which my employer submitted to adjust my visa status to permanent resident (I-485), sent to a USCIS service center, has not been processed after five years. However, my application cannot be processed without the name check by the FBI, which was requested by USCIS three years ago. I thought that USCIS was reducing the processing time for immigration applications? These delays impact families, financially and emotionally. Please assist in my efforts to expedite the processing of my name check."
- **REAL ID** – An individual notes, "I am against the implementation of the REAL ID Act. I believe that it is too intrusive; I resent being asked for my marriage license and social security card."

Although the Privacy Office also receives many telephone inquiries, the Office has only recently begun to keep a record of calls and will report on them in the next Annual Report.

5. Implementation of Privacy

5.1. Managing the Protection of Privacy

Governments collect sensitive PII that can be misused by identity thieves, and must therefore take appropriate steps to ensure that the information is properly protected. Just as private entities need to develop and strengthen their security programs, government agencies must carefully examine their methods of protecting the privacy of individuals whose information they collect and store. While certain privacy protection obligations are imposed by law, others are simply a function of proper oversight and management.

5.2. Privacy Incident Response Policies and Procedures

As the use of IT has grown both in the public and private sector, threats and vulnerabilities to the security and protection of the PII maintained within those information systems has increased exponentially. Paper record systems are not exempt from these vulnerabilities. The Federal Government collects PII from its employees, the American public, and visitors to the United States, which, if not protected adequately, can be misused by identity thieves. The Federal Government must take appropriate steps to ensure that the PII that it collects and maintains is properly protected.

To address the growing concerns about privacy breaches at multiple Federal agencies, on May 10, 2006, the President issued Executive Order 13402, establishing the President's Identity Theft Task Force. In a September 2006 memorandum issued by OMB and in its final April 2007 report, *Combating Identity Theft: A Strategic Plan*, the Task Force issued several recommendations. These recommendations are aimed at ensuring that government agencies take concrete steps to improve their data security measures, and develop incident response procedures that include processes to mitigate the harm caused by a privacy incident, such as issuing notice to affected individuals, when appropriate.

The Privacy Office staff participated in and contributed to the Task Force working groups that focused upon public sector issues.

OMB has issued various guidance documents in response to the recommendations of the Identity Theft Task Force, including OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006), Clay Johnson III's Memorandum to Agency Heads: *Recommendations for Identity Theft Related Data Breach Notification* (September 20, 2006), and OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007). The Privacy Office staff participated in OMB working groups and contributed to the drafting of these memoranda.

Because the majority of privacy incidents involve information technology, OMB M-07-16 calls for an effective response plan that includes the delineation of roles of several entities across the Department. On April 26, 2007, Deputy Secretary Michael Jackson issued a memorandum to all DHS Under Secretaries and Component Heads stating:

> "The Department takes very seriously its responsibilities to safeguard personally identifiable information of its employees, as well as people with whom it does business and interacts…At my instruction, the Privacy Office, with the help of the Chief Information Officer, is drafting Privacy Incident Handling Guidance that will provide a comprehensive response capability for privacy incidents at the Department."

The Privacy Office has collaborated with the DHS CIO, DHS CISO, DHS CSO, and DHS Security Operations Center (DHS SOC) to develop a comprehensive privacy incident response plan to address detection, reporting, escalation, containment, investigation, and notification for privacy incidents ranging from low to high impact of risk of identity theft or harm to affected individuals.

The Privacy Office has led the effort to develop and implement a comprehensive privacy incident handling guidance document for the Department. The DHS Privacy Incident Handling Guidance (PIHG), to be issued in late summer 2007, informs DHS organizations, employees, and contractors of their obligation to protect the PII that they are authorized to handle. The PIHG will establish policies and procedures outlining how DHS components, employees, and contractors must respond to the suspected or confirmed potential loss or compromise of PII[7] and defines the roles and responsibilities of personnel and management in responding to incidents.

A key feature of the PIHG will be that there are established procedures to assess the potential impact of an incident upon affected individuals and the escalation of incident handling to a specified group of Departmental officials. OMB M-07-16 requires a "core

[7] OMB M-06-19 requires agencies to report all suspected and confirmed incidents involving PII to the U.S. Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident. The PIHG is structured to expedite incident reporting as required by OMB M-06-19 and OMB M-07-16.

management group" to convene for review and mitigation of incidents where there is a moderate to high risk of identity theft. The PIHG will require each component to maintain a Component Privacy Incident Response Team (C-PIRT), which is a standing group of component personnel who are designated in advance to handle a moderate-impact level privacy incident on behalf of the component. In addition, DHS will have a Department Privacy Incident Response Team (D-PIRT), a standing group of senior officials from DHS that will convene as needed to handle a high-impact incident on behalf of the Department. The D-PIRT may also be convened to address moderate-impact incidents involving headquarters systems.

Components have already begun the process of implementing the provisions of OMB M-07-16 in advance of the DHS PIHG. TSA recently established a Data Breach Response Team to provide a mechanism for designated TSA personnel to report and monitor the detection or discovery of a suspected or confirmed privacy incident. The Privacy Office is working with other components to develop similar response teams and to implement the provisions of OMB M-07-16 and the PIHG.

The DHS Chief Privacy Officer, in close collaboration with the DHS CIO, DHS CISO, and DHS CSO ensures that all DHS privacy and information security incidents are identified, reported, and that an appropriate response is taken to mitigate harm to DHS-maintained assets and information. While each privacy incident must be evaluated individually, the DHS PIHG will provide DHS components, employees, and contractors with a set of guidelines for assessing a situation and responding to a privacy incident in a timely and appropriate manner.

5.3. Reducing the Use of Social Security Numbers at the Department

The SSN is a particularly sensitive type of PII created for the purpose of administering Social Security and tax laws. Given its unique relation to an individual and role in financial decision-making, any use of an SSN poses additional privacy and security risks, including the growing problem of identity theft.

The Privacy Office is committed to ensuring that SSNs are used by the Department only for appropriate purposes and, when used, that SSNs are maintained and transmitted securely. On June 4, 2007, the Privacy Office issued DHS Privacy Policy Memo 2007-02, *Use of Social Security Numbers at the Department of Homeland Security*. DHS is implementing steps to ensure that SSNs will be used only in limited instances, only where necessary, and any transmission of SSNs will be done via a secure network communication. The Privacy Office is conducting a review of all DHS systems currently collecting, maintain, and using SSNs, to identify where DHS may either eliminate the collection and use of SSNs for a program or where DHS needs to strengthen the security of a system which maintains SSNs.

The Privacy Office has mandated that all new systems will not use SSNs as a unique identifier unless required by law or pursuant to a specific authorized purpose. This data protection program will be an ongoing initiative throughout DHS during the coming year.

5.4. Protecting the Privacy of PII Collected from Non-U.S. Persons

The Privacy Act provides statutory privacy rights to U.S. citizens and Legal Permanent Residents (LPRs); however, the Privacy Act does not provide access or amendment rights to visitors or aliens.

Issued on January 19, 2007, DHS Privacy Policy Guidance Memorandum 2007-01, *Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons,* establishes that any PII collected, used, maintained, and/or disseminated in connection with a "mixed system" by DHS shall be treated as a system of records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, LPR , visitor, or alien. Under the DHS "mixed system policy," non-U.S. persons have the right of access to their PII collected, maintained, retained, and/or disseminated by DHS and the right to amend their records, absent an exemption under the Privacy Act[8]. However, the DHS mixed system policy does not extend or create a right of judicial review for non-U.S. persons.

The DHS mixed systems policy is based on the Privacy Office's statutory responsibility under Section 222(2) of the Homeland Security Act, as amended, to "assure personal information contained in Privacy Act systems of records is maintained in full compliance with fair information principles as set out in the Privacy Act." As the Privacy Office works to integrate the fair information principles into programs and initiatives that support the Department's mission, DHS must ensure that it retains the trust of non-U.S. persons who chose to visit, study, and do business in the United States. The DHS mixed system policy is an important step for the Privacy Office and for DHS.

6. Education and Training

The Privacy Office seeks to provide appropriate training for all DHS employees and contractors regarding privacy and the obligation to protect PII throughout the Department.

6.1. Expanding Awareness through Training

Employee education is a key tool for ensuring that employees are informed about how to handle and protect PII in a responsible and appropriate manner. The Privacy Office has expanded its training offerings to improve employee recognition and understanding of the privacy concerns that may occur within the course of their daily duties and responsibilities. These new offerings include introductory privacy awareness training, web-based training, and in-depth training on privacy compliance issues.

The Privacy Act and Appendix 1 of OMB Circular A-130, *Management of Federal Information Resources* also mandates regular Privacy Act training for employees. Many

---

[8] As stated in OMB's 1975 guidance, Circular A-108 *Privacy Act Implementation: Guidelines and Responsibilities* (July 9, 1975), "Where a system of records covers both [U.S. persons] and [non-U.S. persons], only that portion which relates to [U.S. persons] is subject to the Act, but agencies are encouraged to treat such systems as if they were, in their entirely, subject to the Act." [40 FR 28948]

of the legacy components have existing Privacy Act training courses; the Privacy Office is working with these components to update those training programs as needed.

The Privacy Office provides introductory privacy awareness training to all incoming headquarters employees. This introductory training is presented as part of the new employee orientation session. The Privacy Office also participates in the new employee orientation sessions of several components; the Privacy Office is currently working with the Office of the Secretary to develop a privacy information segment to be included in a DHS-wide orientation program. In addition, the Privacy Compliance group offers privacy compliance training for employees working on privacy documents and other compliance requirements.

Given the large employee population of DHS, the Privacy Office will begin to use technology to ensure Departmental compliance with this important requirement. In addition to the new employee orientation, the Privacy Office has developed and distributed an e-learning privacy training course, "A Culture of Privacy Awareness," which teaches the privacy essentials of the Privacy Act and E-Government Act. This training permits DHS employees and contractors to recognize situations in which privacy issues arise and how to reduce risks to privacy in the development and operation of a program. This course will soon be available across DHS and has already been incorporated into some components' privacy training programs, including USCG and TSA. In the near future, the course will be part of DHScovery, the new Internet-based learning management system for DHS Headquarters employees. In addition, the Privacy Office has shared this training course with other Federal agencies, including the Office of Personnel Management (OPM), DOS, Department of the Navy, Department of the Treasury, and Department of the Interior.

The Privacy Office is nearing the completion of the development of two Privacy Act e-learning courses entitled "Privacy Act 101" and "Privacy Act 201." The initial course, "Privacy Act 101," will provide DHS employees and contractors with the essentials concerning the Privacy Act, including a basic understanding of PII and SORNs, when a SORN is required, how information is collected, used, maintained, or disseminated in compliance with the Privacy Act, and other related topics. Further, it introduces DHS employees and contractors to the fair information principles employed by the Privacy Office. The course addresses employee and contractor responsibilities as well as consequences for non-compliance and violations of the Privacy Act. The second course, "Privacy Act 201," is intended for program managers, developer leads, PPOCs, and departmental supervisors to instruct on management responsibilities concerning the Privacy Act. The Privacy Office is working with the DHS Advanced Distributed Learning Program Management Function (DHS ADL) to make both "Privacy Act 101" and "Privacy Act 201" available through the DHScovery learning management system in the coming months.

6.2. Privacy as Part of Security Awareness Training

In August 2007, the Privacy Office will provide additional privacy training, focusing on how to handle incidents involving PII and an introduction to the requirements of the DHS PIHG, to headquarters employees as part of the annual DHS Security Awareness

Training conference. Training for handling privacy incidents involving PII is required by OMB M-07-16.

6.3. Workshops

On November 28-29, 2006, DHS co-hosted the second International Conference on Biometrics and Ethics in Washington, DC. This conference brought together approximately eighty (80) experts from several countries to engage in an open discussion of the application and ethics of biometrics.

As mentioned above, the Privacy Office updated and re-issued its *Privacy Impact Assessment Guidance* in May 2007. On May 23, 2007, Privacy Office staff conducted a workshop where almost two hundred (200) Federal employees and contractors were trained on privacy awareness and developing PIAs.

6.4. Staff Training and Certification

The Privacy Office believes strongly in continuing education to stay abreast of developments in privacy law and policy. All Privacy Office subject matter experts, including the Chief Privacy Officer, sat for the accreditation examination of the International Association of Privacy Professionals (IAPP) to receive both the Certified Information Privacy Profession (CIPP) accreditation and the government-sector privacy accreditation (CIPP/G). In addition to the accreditation examination preparatory course, the maintenance of the CIPP and CIPP/G accreditations requires each member of the Privacy Office to participate in at least ten (10) hours of continuing professional education in the privacy field each year.

Also, the DHS Privacy Office is working with component privacy officers and PPOCs to make Departmental privacy training resources, such as the Privacy Awareness web-based training course, available to components and programs to increase privacy awareness in all DHS employees and contractors.

In June 2007, the Chief Privacy Officer and members of the senior staff attended the Third Intelligence Law Course at the Judge Advocate General's Legal Center & School in Charlottesville, Virginia. The course introduces new practitioners to the field of intelligence law; provides a basic understanding of the legal framework in which the intelligence community operates and the historical context with which to view, understand, and apply existing laws, regulations, and policies; and provides an overview of the organization, roles, and functions of the intelligence community.

The training strengthens the Privacy Office's understanding of intelligence law, which is important given that the Privacy Office is working more closely with the DHS Office of Intelligence and Analysis (DHS I&A) on such programs as the Department's State and local Fusion Center program.[9]

[9] The DHS Fusion Center program was established to provide a mechanism for bi-directional sharing of criminal/terrorism related intelligence between State, local, and tribal partners and various agencies within the Federal government..

In support of continuing education, the Privacy Office budgets appropriate resources for training, which Privacy Office staff are encouraged to use to the fullest in order to ensure that important privacy skills are kept up-to-date.

7. Outreach

7.1. Public Outreach and Presentations

A key component of the Privacy Office's outreach efforts involves the DHS Chief Privacy Officer and senior staff participating in a wide variety of public events. Throughout this year, the Privacy Office has participated in almost two dozen events covering such diverse topics as privacy and security, biometrics, identity theft, RFID technology, credentialing and identification management, and privacy compliance.

7.1.1. Congress

During this reporting period, the DHS Chief Privacy Officer has continued to brief Congress and its staff on the work of the Privacy Office. During this time, the DHS Chief Privacy Officer offered testimony at two subcommittee hearings and visited with Members of Congress, their staffs, or Committee staff on five occasions.

The Chief Privacy Officer first testified on March 14, 2007, before the House Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment about privacy and civil liberties within the DHS Fusion Center program. The Chief Privacy Officer spoke about DOJ's *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (August 2006), developed in collaboration with DHS, saying, "the guidelines promote meaningful and lawful privacy policies . . .and provide mechanisms ensuring that the [fusion] centers adhere to these policies." He also called the guidelines "an invaluable resource" for fusion center operators.

The Chief Privacy Officer next appeared before Congress on March 21, 2007, before the House Appropriations Committee Subcommittee on Homeland Security at a hearing on enhancing privacy and civil rights while meeting homeland security needs. Here, the Chief Privacy Officer discussed the Privacy Office's mission and its responsibilities, the Office's FY 2008 budget request, and its privacy and FOIA compliance operations. "The Privacy Office stands ready to address the next set of challenges," Mr. Teufel told the Subcommittee.

Most recently, the Chief Privacy Officer testified on July 24, 2007, before the House Judiciary Subcommittee on Commercial and Administrative Law about the Privacy and Civil Liberties Oversight Board and his role as DHS's Chief Privacy Officer. The Chief Privacy Officer told the Subcommittee that, "the hard work of my compliance staff" contributed to the "substantial progress in both the number and, significantly, the quality of privacy impact assessments issued by our office… I'm confident [our continued] efforts will support the trend."

In addition to offering testimony, the Chief Privacy Officer reached out and responded to requests from Members and Committee staff. Over the past year, the Chief Privacy

Officer and senior staff have visited with U.S. Representative Christopher Carney, Chairman of the House Homeland Security Committee Subcommittee on Management, Investigations, and Oversight; attended a member briefing with Representative Sheila Jackson-Lee of the House Homeland Security Committee; briefed Committee staff from the House Homeland Security Committee on the ISE, and later, WHTI; and briefed Committee staff from the Senate Homeland Security and Governmental Affairs on the Privacy Office's major activities.

7.1.2. Communication with Privacy Groups

The Chief Privacy Officer and senior staff regularly meet with privacy organization leaders to listen to their concerns and better understand what issues are of importance to their constituencies. During this reporting period, senior staff have met or held conference calls with representatives from the ACLU, CDT, EPIC, and the Electronic Frontier Foundation.

The public meetings of the Data Privacy and Integrity Advisory Committee (DPIAC) provide opportunities for privacy groups and the public to hear from the Privacy Office and DHS representatives on issues surrounding policy and operational issues and how those issues impact privacy and are addressed. These meetings also provide for public comment either through written submissions or the ability for the public to address the Committee directly at the meeting. The Privacy Office often asks members of the privacy community to participate as panelists and subject matter experts at DPIAC meetings. During this reporting period, staff members from the ACLU, CDT, and EPIC have participated as panelists at a DPIAC meeting.

7.2. Privacy Matters

Since 2005, the Privacy Office has produced a newsletter entitled, *Privacy Matters,* which seeks to inform our DHS colleagues, Members of Congress, our international partners, and the privacy community at-large of the important work of the office within the Department. The newsletter is available in hard copy, electronically, and via the Privacy Office website at www.dhs.gov/privacy. Given the newsletter's broad audience, *Privacy Matters* is an important part of the Privacy Office's outreach program.

Topics featured in *Privacy Matters* over the summer 2006, fall 2006, winter 2007, and spring 2007 include:

- Promoting privacy protections in the DHS investment review process;
- Highlights of meetings of the DPIAC;
- PIA tutorial workshops;
- Privacy Office improving DHS FOIA;
- Privacy Office issues updated PIA Guidance;
- International outreach; and
- Privacy Office news, including new staff members and initiatives.

8. Interagency Contributions to Privacy

8.1. Information Sharing Environment

Section 1016 of the IRTPA required the Federal Government to implement a recommendation of the 9/11 Commission to create a new means and methodology to share terrorism information across the entirety of the Federal Government as well as State, local, tribal, and foreign governments and private sector entities. Furthermore, the statute created a Program Management Office for the development and implementation of the Information Sharing Environment (PM/ISE) within the Office of the Director of National Intelligence (ODNI). On October 25, 2005, the President issued Executive Order 13388, which outlined particular requirements for the ISE and required the PM/ISE to coordinate with various members of the Federal Government to begin the work necessary to draft the Implementation Plan as required under IRTPA.

At the time of the Executive Order, the PM/ISE initiated Coordinating Group meetings for various subject matters including Search, Exploitation, and Access issues [technology implementation], Collaboration and Governance, and Security and Privacy. The DHS Privacy Office participated in all Coordinating Group activities to provide privacy leadership, support Departmental goals, and coordinate with other parts of the Department. The output of these Coordinating Groups was used by the PM/ISE to advise the President for the drafting of the Presidential Memorandum, *Guidelines and Requirement in Support of the Information Sharing Environment*, issued December 17, 2005, setting forth specific guidelines for development of the ISE.

Out of these guidelines, working groups were developed with agency leads to develop privacy guidance. Throughout the year, the Privacy Office participated on a number of groups, including the Guideline 5 Privacy Group, the Controlled Unclassified Information (CUI) group, Foreign Government Information (FGI) group, and the State, Local, Tribal, and Private Sector group.

The Privacy Office has been an active participant in developing an inter-agency ISE as well as the internal DHS efforts to develop information sharing procedures. The Privacy Office's Director for Privacy Technology is an active member of the Department's Information Sharing Coordinating Council (ISCC), which brings representatives from across the Department together to address information sharing issues and support the Department's overall participation in the ISE.

The Privacy Office was invited by the ODNI and DOJ to participate in a core working group to do the initial development of the privacy guidance as required under Guideline 5 of the Presidential Memorandum. The President issued the final *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* ("Privacy Guidelines") at the end of 2006. The Privacy Office is a member of the ISE Privacy Guidelines Committee and serves as the co-chair of the State, Local, and Tribal Working Group of the Committee along with the Privacy and Civil Liberties Office of the FBI.

8.2. White House Privacy and Civil Liberties Oversight Board

The Privacy and Civil Liberties Oversight Board was recommended by the 9/11 Commission and established by the IRTPA. It consists of five members appointed by and serving at the pleasure of the President. The Board advises the President and other senior executive branch officials on issues concerning privacy and civil liberties and works to ensure that these are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. This includes advising on whether adequate guidelines, supervision, and oversight exist to protect these important legal rights of all Americans.

The Chief Privacy Officer and Privacy Office senior staff have frequently met with Privacy and Civil Liberties Oversight Board Executive Director Mark Robbins to discuss Federal privacy issues. Furthermore, in September 2006, Robbins appeared before the DHS DPIAC, providing a summary of the board's activities since its inception.

8.3. OMB Interagency Privacy Committee

The Privacy Office was an original participant in the Interagency Privacy Committee chaired by OMB. In May 2007, OMB restructured the monthly forum as a full committee of the CIO Council. The Privacy Committee will continue to serve as a forum for agency privacy officers to exchange views and information on issues of mutual concern, including the sharing of privacy best practices government-wide. This past year, the interagency group has focused on developing guidance for establishing safeguards to prevent and respond to breaches involving PII and best practices for privacy incident handling.

8.4. President's Identity Theft Task Force

Through Executive Order 13402, issued on May 10, 2006, the President established an Identity Theft Task Force comprised of seventeen (17) Federal agencies, including DHS. The mission of the Task Force was to develop a comprehensive national strategy to combat identity theft. In the Executive Order, the President specifically directed the Task Force to make recommendations on steps the Federal Government can take to reduce the likelihood of identity theft.

In its preliminary recommendations, issued in September 2006, and its subsequent April 2007 Strategic Plan, *Combating Identity Theft: A Strategic Plan*, the Task Force made several recommendations aimed at ensuring that government agencies take concrete steps to improve their data security measures. The Task Force recommended that OMB and DHS outline best practices in the arena of automated tools, training processes, and standards that would enable agencies to improve their security and privacy programs. The Task Force also recommended the development of a list of the most common mistakes to avoid in protecting PII held by the government. DHS contributed to the mission of the President's Task Force by serving as a member of the Task Force as required by Executive Order 13402; providing comment and feedback on draft guidance; and contributing to discussions on the Task Force's work groups.

As recommended by the Task Force, the Privacy Office is taking the lead within the Department to develop appropriate policies and handling practices for PII and is working with components and programs to improve privacy protection programs. In addition, as mentioned above, the Privacy Office is leading the development of the DHS PIHG, which will serve as a model to other Federal agencies as they develop their own privacy incident response procedures.

9. Data Privacy and Integrity Advisory Committee

The DPIAC provides advice and guidance to the Secretary and the Chief Privacy Officer on programmatic, policy, operational, and technological issues within DHS that relate to PII, as well as data integrity, and other privacy-related matters.

The DPIAC was formed at DHS in 2004 under the authority of the Federal Advisory Committee Act [5 U.S. Code Appendix 2]. Members come from large and small companies, academia, and the non-profit sector, and are selected because of their expertise, education, training, and experience in the fields of data protection, privacy, and/or emerging technologies.

During this reporting year, the Committee held four public meetings, and issued three reports.

- In September 2006, the Committee met at TSA headquarters in Arlington, Virginia. The meeting featured remarks by DHS Deputy Secretary Michael Jackson, who said it was very helpful to the Department to have an advisory committee focused on privacy issues. The Committee also heard from Mark Robbins, the executive director of the Privacy and Civil Liberties Oversight Board, who discussed the Board's mission. The meeting included a discussion of screening programs at DHS, with then TSA Special Counselor Tamara Miller discussing TSA screening programs and Director Kathleen Kraninger highlighting the work of the DHS Screening Coordination Office.

  The Committee also had two other panels on data integrity and on redress. The data integrity panel included Jennifer Barrett of Acxiom, Steve Page of Trans Union, and Xuhui Shao from ID Analytics. The redress panel featured the TSA Redress Office's James Kennedy and Debra Rogers from the USCIS Customer Service Office.

- In September 2006, the DPIAC re-organized into four subcommittees:
  - Data Integrity and Information Protection Subcommittee;
  - Privacy Architecture Subcommittee;
  - Data Acquisition and Use Subcommittee; and
  - Administration Subcommittee.

- The Committee held its December 2006, meeting in Miami, Florida. At this meeting, the Committee approved two reports, *The Use of RFID for Human Identity Verification* and *The Use of Commercial Data*. The first report presents an analytical framework for the Department to use in determining whether to

deploy RFID technology, and offers a set of best practices to consider when DHS chooses to use RFID technology. The second report, which updates the Committee's October 2005 report, *The Use of Commercial Data to Reduce False Positives in Screening Programs*, presents recommendations on policies and procedures for limiting access to commercial data by public agencies and provides guidance to the DHS Privacy Office on the use and management of commercial data.

In addition, the Committee heard presentations on maritime infrastructure, privacy at TSA, the WHTI, international perspectives, data integrity, and DHS FOIA operations. Participants included the Honorable Jennifer Stoddart, Privacy Commissioner of Canada; Rear Admiral Joseph L. Nimmich, USCG; Peter Pietra, Director of Privacy Policy and Compliance at TSA; John Wagner, Director of Passenger Automation Programs, Office of Field Operations, CBP; Dr. John Talburt of the University of Arkansas-Little Rock; and Catherine Papoi, DHS Deputy Chief FOIA Officer.

- In March 2007, the Committee began its third year, meeting again at TSA headquarters in Arlington, Virginia. The meeting featured remarks on REAL ID by DHS Assistant Secretary for Policy Stewart Baker. The committee also heard from two panels: one on the DHS REAL ID rulemaking and the other on outside perspectives. Participants in the REAL ID panels included Jonathan Frenkel, Senior Policy Advisor, DHS Office of Policy; Selden Biggs, Director, REAL ID Program Office; David Quam of the National Governors Association; Barry Steinhardt from the ACLU; Anne Collins, Registrar of Motor Vehicles, Commonwealth of Massachusetts; Sophia Cope from the CDT; Melissa Ngo of EPIC; and Robert Burroughs, Assistant Chief, Texas Department of Public Safety.

  In addition, the Committee hosted two panels featuring DHS officials, one on IT transformation within USCIS, and the other on data integrity and records retention within DHS. Participants in the two panels included Daniel Renaud, Chief, USCIS Transformation Program Office; Gerri Ratliff, Chief, USCIS Verification Division; Dominick Gentile, Chief, USCIS Records Division; and Kathy Schultz, Senior Records Officer for DHS Records Management.

- In May 2007, the Committee met again at TSA headquarters in Arlington, Virginia, to consider issuing a report on the REAL ID NPRM. As a result of the meeting discussion, the Committee issued a report to the Chief Privacy Officer and DHS Secretary that included twelve recommendations on the implementation of REAL ID. The recommendations addressed such topics as security safeguards, privacy safeguards, storing PII in the machine readable zone of the card, access to the States' driver's license databases, and background checks for employees involved in the manufacturing and production of REAL ID licenses.

All DPIAC reports and meeting notes are posted on the Committee website at www.dhs.gov/privacy.

10. International

The Privacy Office provides crucial policy and programmatic guidance to the Secretary and DHS components on international privacy matters. During this reporting period, the Privacy Office continued to expand its reach and effectiveness within the Department and with its partners abroad.

10.1. Assisting with International Issues

Many of the Department's cross-border efforts involve information sharing and other data privacy issues with foreign governments and regional organizations. When the United States – European Union (U.S.–E.U.) Agreement on PNR, in effect since 2004, was overturned by the European Court of Justice in May 2006, the DHS Policy Office led negotiations for an interim and a final agreement. As experts on international privacy frameworks, the Privacy Office was an important resource to the DHS negotiating team as it worked toward another agreement pending the July 2007 expiration of the existing PNR agreement. Negotiating within the U.S.–E.U. High Level Contact Group (HLCG) on privacy principles involving law enforcement and public security, described in detail later in this section, involved close collaboration between the Privacy Office staff and with other DHS components and interagency offices.

In many cases, international issues are closely integrated with other activities within the Privacy Office. For example, international expertise has assisted the Privacy Compliance Group's review of PIAs for programs and initiatives with international facets. Privacy guidance, including DHS Privacy Policy Guidance Memorandum 2007-01 has been enhanced by international considerations. The Privacy Office has provided advice and comments to several components as they pursued numerous bilateral and multilateral arrangements and agreements.

10.2. Working with the International Community

The Privacy Office represents the Department in the international privacy community. A primary goal of the Privacy Office's international activities is to convey to the global community the importance of the fair information principles, and to influence emerging international privacy standards.

Because national security issues do not necessarily recognize national borders, information exchanges with the Department's international partners are critical to support the DHS mission. In order to develop and influence policy and practice in the international privacy field, DHS must fully participate in regional initiatives and multi-lateral organizations. In a number of outreach activities this year, the Privacy Office promoted the U.S. privacy framework as an effective way to protect PII while not impeding trans-border data flows and the national security programs that depend on such information. The Chief Privacy Officer and the International Privacy Policy group have met with their counterparts in Canada, Belgium, Germany, the United Kingdom, Switzerland, France, Australia, and Singapore.

The Privacy Office's international outreach efforts include participation in multilateral global forums, such as the Organization for Economic Cooperation and Development

(OECD) and the International Conference of Data Protection and Privacy Commissioners. The Privacy Office also concentrates its work on issues with the E.U., as well as within region-centric international organizations, such as the Asia Pacific Economic Cooperation (APEC).

During the reporting period, the Privacy Office represented the Department and DHS privacy policies at the following international forums:

10.2.1. The International Conference of Data Protection and Privacy Commissioners

The 28th annual International Conference of Data Protection and Privacy Commissioners, which took place in London, United Kingdom, in November 2006, is an important annual event for the global privacy community. The conference brought together national data protection authorities from around the world and representatives of business and government sectors, as well as members of the public, for a discussion of issues relevant to privacy and data protection. This conference provided the International Privacy Policy group with an opportunity to further communicate with and inform the U.S.'s global partners of U.S. interest in privacy protection and privacy values, which in turn, improves the U.S. Government's ability to work with international partners on cross-border data sharing. Traditionally, the last day of the conference is a closed session reserved for accredited representatives of government data protection authorities. Since 2004, the DHS Privacy Office has had "Observer" status in the conference, which allows admittance and participation in closed meetings of the conference. This status is a recognition and acknowledgment on the part of the international community of the leadership role played by the DHS Privacy Office in shaping privacy policy within the U.S. Government. DHS's International Privacy Policy group, together with a representative of the Federal Trade Commission (FTC), the Chief Privacy and Civil Liberties Officer of DOJ and the Vice Chairman of the Privacy and Civil Liberties Oversight Board represented the U.S. Government at this November 2006 event.

The next International Conference of Data Protection and Privacy Commissioners will be hosted by the Canadian Privacy Commissioner in September 2007. The theme of this upcoming conference will focus on the shifting privacy landscape and the interactions of technology and privacy. In recognition of DHS's leadership and outreach efforts, the Canadian Privacy Commissioner invited the Privacy Office to present as well as to suggest other agenda topics and speakers.

10.2.2. The Organization for Economic Cooperation and Development

The Privacy Office continued to participate in OECD's work on cross border privacy enforcement. The effort, lead by the Canadian delegation, is intended to focus on privacy law enforcement for consumers and industry. The Privacy Office's ongoing participation ensures that OECD's work does not affect government-to-government PII sharing or cases where PII would be used by the U.S. Government in a cross-border arrangement, such as in situations similar to PNR exchanges of information. In working with other members of the OECD Working Party on Information and Privacy (WPISP), including the Secretariat, DHS's International Privacy Policy group was able to make changes to the group's draft recommendation, which should protect DHS equities on cross-border

information sharing. With the work led by the Canadians in both the OECD and the International Conference of Data Protection and Privacy Commissioners, the Privacy Office expects that cross-border privacy enforcement will be an important topic during the conference this September in Montreal.

10.2.3. International Association of Privacy Professionals

In October 2006, the Chief Privacy Officer made his first official international appearance at the IAPP annual summit in Toronto, Canada. The Chief Privacy Officer met with Canadian Privacy Commissioner Jennifer Stoddart and Ontario Privacy Commissioner Ann Cavoukian and addressed IAPP members at the speakers' dinner.

10.3. Regional Initiatives

10.3.1. European Union

As referenced above, DHS has engaged with the E.U. in ongoing discussions on data sharing, as well as on specific data sharing agreements. The Privacy Office has served as a resource and participant in discussions under the HLCG, established November 6, 2006, by the U.S.-E.U. Justice and Homeland Affairs Ministerial. The goal of the HLCG is to develop a comprehensive framework under which law enforcement and public security information can be transferred without *ad hoc* negotiations of data protection laws in connection with each such transfer.

Additionally, the Privacy Office has worked with DOJ, DOS, and other DHS components on a draft agreement between Germany and the U.S. for *Querying Fingerprint and DNA Databases and the Exchange of Information to Combat Terrorism and Serious Crime*, otherwise known as the Prüm Agreement. This agreement aims to improve cooperation between each country's competent authorities in criminal investigations and prosecutions and in the prevention of terrorism and other serious crime. The Privacy Office's focus is to ensure that appropriate data privacy provisions are embedded in the final agreement.

The Privacy Office has reached out to European audiences through speaking engagements at the European Institute and the German Marshall Fund in Washington to educate the Europeans on U.S. privacy policy. Additionally, the International Privacy Policy group participated in a conference on International Transfers of Personal Data in Brussels, Belgium, which was co-sponsored by the U.S. Department of Commerce and the E.U. Article 29 Working Party. Bilateral meetings with the Article 29 Working Party were held to discuss issues pertaining to PII in law enforcement/national security efforts.

From May 7-11, 2007, the Chief Privacy Officer, supported by the Director of International Privacy Policy, traveled to Brussels to meet with members of the international and European media as well as E.U. government officials that included the European Data Protection Supervisor; members of the Freedom, Security and Justice Directorate of the Commission; and members of the European Parliament. The visit also involved a full day of discussions for the High Level Contact Experts Group, mentioned earlier in this section. This trip included a meeting with the [German] University of Konstanz's Professor Kay Hailbronner, public outreach with the Swiss media, and a meeting with the Swiss Data Protection Authority. The trip provided an ideal opportunity

for the Chief Privacy Officer to present the U.S. privacy framework and build useful relationships with European data protection authorities.

From June 11-15, 2007, the Chief Privacy Officer, supported by the Director of International Privacy Policy, traveled to Berlin and Paris to meet with members of the international and European media; data protection authorities; representatives from the German Ministry of the Interior and Chancellery; and non-governmental organizations involved in data privacy. In addition, the Chief Privacy Officer's meetings with data protection counterparts also provided greater understanding of German and French data protection frameworks. The trip provided the Chief Privacy Officer with an opportunity to discuss U.S. privacy frameworks with his European counterparts and to build vital relationships with European data protection authorities. The Chief Privacy Officer used these meetings to introduce the Department's mixed system policy and DHS TRIP and to emphasize the extension of administrative privacy protections to non-U.S. citizens.

10.3.2. Asia Pacific Economic Cooperation

In September 2006, the Privacy Office made a presentation to the APEC E-Commerce Steering Group on DHS's development of PIAs. The Privacy Office also participated in drafting privacy provisions in the Regional Movement Alert System (RMAS). The resulting MOU was adopted as a model by the APEC Business Mobility Group and endorsed by the APEC Ministers.

In January 2007, the Privacy Office participated in the APEC Electronic Commerce Steering Group's (ECSG) Data Privacy Subgroup (DPSG) meeting in Canberra, Australia, where participants agreed upon a model for the commercial cross-border exchange of PII. DHS supported the "flexible model," which is not tied to a particular legal structure and sets an important precedent for future international data sharing mechanisms. The Privacy Office remains engaged in APEC activities to ensure that the scope of discussions does not jeopardize data sharing in the national security/law enforcement context.

10.4. International Outreach

10.4.1. Biometrics

The Privacy Office co-hosted an International Conference on Biometrics and Ethics with US-VISIT and the DHS Biometric Coordination Group, November 28-29, 2006, in Washington, D.C. This conference was held to promote understanding and international cooperation on the use of biometrics as its technologies evolve and impact individuals' privacy. The conference brought together approximately eighty (80) experts from several countries to engage in an open discussion of the application and ethics of biometrics.

Participants included representatives from academia, private industry, non-profit organizations and government, and hailed from Asia, Europe, the Middle East, and North America. In addition to DHS, representatives from the Department of Defense (DOD), DOJ, and DOS also attended.

Several themes emerged from the two days of discussion, including the critical need to study and develop guidance for biometrics use, the need to apply fair information

principles to biometrics, and the potentially long-lasting implications of biometrics on societies and individuals. The conference set the groundwork for a possible third conference to further discuss the ethical issues of biometrics use for security purposes and identity management.

10.4.2. Aviation, Singapore

On January 29-30, 2007, the Director of International Privacy Policy attended a two-day conference on Aviation Security in Singapore. More than fifty (50) officials from the aviation security branches of Asian, Canadian, and Middle Eastern governments attended, along with private representatives from the aviation industry.

The Director presented an overview of DHS and its use of PII relevant to aviation security. He also discussed developments in the E.U. and Asia Pacific region and suggested a global strategy for resolving impediments to the free flow of information for law enforcement and national security purposes.

The Director's participation set the foundation for further contacts with Singaporean data protection officials, who expressed a willingness to share developments in their privacy work.

11. Reports

11.1. ADVISE Report

In July 2007, the Privacy Office released the *ADVISE Report: DHS Privacy Office Review of the Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE) Technology*. The Privacy Office conducted its review of the DHS S&T Directorate's technology initiative pursuant to Section 222(2) and (6), of the Homeland Security Act of 2002, as amended, which designates the Chief Privacy Officer as the DHS senior official responsible for ensuring that PII is used in full compliance with the fair information principles of the Privacy Act and for reporting complaints of privacy violations.

The report provides a discussion of the Privacy Office's privacy compliance requirements and the ADVISE technology framework, followed by an examination of ADVISE deployments (implementation of the technology framework). This report concludes with short- and long-term recommendations for responsive action.

The Privacy Office's review of the ADVISE deployments focused on two issues: (1) whether the ADVISE deployments complied fully with the existing privacy compliance requirement to conduct a PIA prior to using PII; and (2) whether the ADVISE deployments used or generated data that were contained in existing systems of records maintained under duly published SORNs as required by the Privacy Act. The Privacy Office review determined that some of the ADVISE deployments did not conduct PIAs. In contrast, ongoing ADVISE deployments are drafting PIAs, as necessary, prior to using PII. Finally, the ADVISE deployments did use or generate data that were contained in existing systems of records maintained under duly published SORNs as required by the Privacy Act.

Based on the nature of the ADVISE technology framework, the Privacy Office determined that the most effective and efficient method of integrating privacy protections into the ADVISE technology framework was to develop a new type of privacy guidance – one that could be adapted to match the architecture of the framework itself. The Privacy Office's guidance document, the *Privacy Technology Implementation Guide (PTIG)*, will provide step-by-step guidance to integrate privacy compliance requirements into the development process for operational systems, including individual deployments of the ADVISE technology framework. The PTIG will address general technology development across the Department. Upon completion of this general PTIG, the Privacy Office will coordinate with DHS S&T to develop a specific PTIG for the ADVISE technology framework.

11.2. Data Mining Reports

In July 2006, the Privacy Office released *Data Mining Report: DHS Privacy Office Response to House Report 108-774.* As the title implies, the report was completed pursuant to House Report 108-774: *Making Appropriations for the Department of Homeland Security for the Fiscal Year ending September 30, 2005, and for Other Purposes*. The July 2006 Data Mining Report includes a definition and description of the process of data mining and sets out the privacy and civil liberties concerns raised by the use of data mining technologies for homeland security. It identifies specific data mining activities and programs at DHS and provides information related to their purpose, data sources, and deployment dates. The report also describes the policies, procedures, and guidance that apply to each data mining activity identified. Looking forward, the report made a number of recommendations regarding DHS data mining activities aimed specifically at addressing the privacy concerns those activities may raise.

The House of Representations House Report 109-699 – *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes,* requested the Privacy Office to prepare a second report on data mining. The 2007 *Data Mining Report*, released in July 2007, provides Congress with updated information about DHS data mining activities. It identifies data mining activities that have been under development or deployed since the July 2006 report. It also reports on the Privacy Office's initial efforts to promote adoption and implementation of the privacy recommendations outlined in the July 2006 report. As the recommendations set out by the Privacy Office have been available to data mining programs for only a short time, this document serves as a status report rather than as a final assessment of the extent and success of their implementation.

11.3. MATRIX Report

In December 2006, the Privacy Office released *MATRIX Report: DHS Privacy Office Report to the Public Concerning the Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project.* The report was completed pursuant to the Chief Privacy Officer's responsibility to report on complaints and inquiries regarding possible privacy violations under Section 222(6) of the Homeland Security Act, as amended. The Privacy Office conducted its review of the MATRIX pilot project, and the role of DHS in the program, in response to a request by the ACLU.

Although the MATRIX program has now been discontinued, the Privacy Office's review illuminates several lessons to be learned from the program that are applicable to any program involving the collection and use of PII. Overall, the Privacy Office found that the MATRIX pilot project was undermined, and ultimately halted, because it did not have a comprehensive privacy policy from the outset to provide transparency about the project's purpose and practices and protect against mission creep or abuse.

11.4. Secure Flight Report

In December 2006, the Privacy Office released *DHS Privacy Office Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations*. The report was completed pursuant to the Chief Privacy Officer's responsibility to report on complaints and inquiries regarding possible privacy violations under Section 222(6) of the Homeland Security Act, as amended. The review was undertaken following notice by the TSA Privacy Officer of preliminary concerns raised by GAO that, contrary to published privacy notices and public statements, TSA may have accessed and stored PII from commercial sources as part of its efforts to fashion a passenger prescreening program.

The Privacy Office review included a thorough examination of documents as well as extensive interviews with TSA personnel and TSA contractors. The review determined that there were areas for needed improvement in operations to better safeguard individual privacy and strengthen public trust in the Secure Flight program.

Given the disparity between the initial published Privacy Notices that explained the commercial data test for Secure Flight and the actual testing program that was conducted, closer consultation and better coordination between the Secure Flight program office and TSA legal, policy, and privacy offices was needed.

To TSA's credit, after being informed of the discrepancy between the published notice and the actual testing program, TSA expressly prohibited the commercial entities involved in testing from maintaining or using the PNR for any purpose other than for Secure Flight testing; in addition, it instituted real-time auditing procedures and strict rules for TSA access to the data. In addition, the TSA Privacy Officer assisted the Secure Flight program with the preparation and submission of a Secure Flight NPRM, SORN, and Privacy Act Exemption NPRM to OMB.

12. Freedom of Information Act

In accordance with Executive Order 13392, *Improving Agency Disclosure of Information*, signed by President Bush on December 14, 2005, DHS Secretary Chertoff designated Hugo Teufel III as the DHS Chief FOIA Officer. Given that FOIA is a pillar of the U.S. privacy protection framework, Mr. Teufel's oversight of both privacy management and FOIA management allows for greater transparency of DHS operations.

As part of his strategy to integrate FOIA within the DHS Privacy Office, Mr. Teufel appointed a Deputy Chief FOIA Officer and Director of Departmental Disclosure and FOIA. The DHS FOIA office also has three full-time employees in the positions of

Associate Director of Operations, Associate Director of Policy and Program Development, and a Senior FOIA Analyst.

12.1. Compliance with Executive Order 13392

In response to the deliverables required by Executive Order 13392, the DHS FOIA office has drafted two DHS improvement plans. The first FOIA Improvement Plan, released in summer 2006, provides a general overview of DHS FOIA operations. In January 2007, the DHS FOIA office released a revision of the first plan, which updates specific activities to eliminate or reduce the FOIA backlog, including changes to streamline FOIA processing and activities to increase public awareness. The revised FOIA Improvement Plan contains concrete milestones, specific timetables, achievable outcomes, and metrics to measure success, while also focusing on particular components with large backlogs. In furtherance of the Executive Order mandate to make FOIA programs more citizen-centered, the DHS FOIA Office implemented an improved, customer-friendly FOIA webpage, assigned FOIA Officers to additional DHS headquarters' programs, appointed its primary FOIA Liaison at the headquarters level, and initiated drafting the final DHS FOIA regulations.

12.2. Intra-Departmental Compliance and Outreach

The Chief FOIA Officer and the Deputy Chief FOIA Officer pay additional attention to the DHS components with the highest backlog numbers, in particular, the USCIS FOIA program. In addition to visiting the USCIS processing headquarters in Missouri multiple times, the DHS FOIA leadership continues to assist USCIS in designing program improvements to decrease their backlog by increasing productivity via personnel and technology. To support the component FOIA programs, the Chief FOIA Officer identified FOIA tracking software for the Department and offered training for the component FOIA personnel.

The Deputy Chief FOIA Officer represents the Department at quarterly meetings of the DOJ's Office of Information and Privacy's (OIP) FOIA Officers Homeland Security Information Group (FOHSIG). This is a working group convened by DOJ OIP 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.

The DHS Privacy Office meets regularly with representatives from the information access community as well as immigration attorneys and advocates. The Deputy Chief FOIA Officer spoke at the 2007 American Immigration Lawyers Association (AILA) annual conference to discuss FOIA within the Department.

12.3. Annual FOIA Report to DOJ

As a relatively new agency of significant size and scope, DHS programs and policies have been and continue to be the subject of numerous FOIA requests because of high public interest in its operations. FY 2006 incoming requests numbered one hundred and thirty-seven thousand, eight hundred and seventy-one (137,871). The Department's

FOIA Program, which is centralized for purposes of establishing policy, but managerially and operationally decentralized in each component, consists of two hundred and forty-one (241) full-time FOIA/Privacy Act personnel and costs an estimated $27 million.

During the reporting period, the Department's FOIA leadership 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 coordinating Department-wide responses.

Concurrent with policy and program development activities, the Privacy Office FOIA staff processed FOIA requests for DHS headquarters programs, including 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 one thousand, one hundred and seventy-four (1,174) initial requests from July 2006 through July 2007. While over half of those requests were transferred to various DHS components, the remaining requests were processed by the Privacy Office FOIA staff. Due to the dedication of the DHS FOIA staff, DHS headquarters has eliminated its FOIA backlog.

In the FY 2006 annual FOIA report, DHS included updated Department FOIA performance information. DHS will continue to provide similar information in its 2007 and 2008 annual FOIA reports to DOJ.

13. Upcoming Challenges and Opportunities

This past year has presented numerous opportunities to continue the Privacy Office mission of ensuring privacy protection while developing new management and oversight programs. 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 awareness, data security, and oversight, into the ways in which DHS components and programs handle PII as these components and programs carry out the Departmental mission. At the same time, these challenges provide opportunities for the Department and the Privacy Office to take the lead in privacy awareness.

13.1. Component Privacy Officers

The designation of privacy officers within each component is a high priority for the Privacy Office. While the Privacy Office retains expertise in all types of privacy issues, the overall mission of the Privacy Office is increasingly demanding. The component privacy officers will report to the component head, but will coordinate with the Privacy Office for privacy compliance and Department-wide initiatives. The long-term goal of the Privacy Office is for each component privacy officer to prepare all privacy

documentation (PTAs, PIAs, and SORNs) at the program or system development level, provide the first stage review at the component privacy level, and then have the DHS Privacy Office conduct the final review to approve the privacy documentation. The component privacy officers will also be responsible for managing other privacy compliance programs as mandated by the DHS Privacy Office.

13.2. Information Sharing Environment Inter-agency Development

The Privacy Office is an active participant in developing an inter-agency ISE. Privacy guidelines have been developed within the *Information Sharing Environment Implementation Plan*, a cooperative effort between the DHS CIO, DHS OGC, DHS CRCL and Chief Privacy Officer. This plan implements a structured plan for identifying and assessing the applicable laws, executive orders, policies, and procedures for sharing "sensitive and/or protected information" consisting of terrorism, homeland security information or law enforcement information. The Privacy Office will continue to participate in the Department's Information Sharing Governance Board.

13.3. Continuing to Build Privacy Protections into DHS Programs and Initiatives

The Privacy Office will continue to require the development of PTAs, PIAs, and SORNs for systems that collect, use, and maintain PII. In addition, the Privacy Office will continue to participate in Departmental rulemakings to ensure that DHS programs and initiatives incorporate privacy protections into program development and decision-making.

13.4. Reducing FOIA Backlogs in DHS Components

DHS FOIA management will continue to address FOIA backlogs across the Department and to improve efforts to manage and address continuing increases in FOIA requests received by the largest components within the Department. The Chief FOIA Officer and Deputy FOIA Officer are working with component leadership to devote adequate resources to their FOIA programs.

14. Appendix: Summary of Privacy Impact Assessments and Systems of Records Notices

14.1. Privacy Impact Assessments

Component	Name of System	Date Approved
NPPD/US-VISIT	United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Aliens	12-Jul-06
CBP	ITDS/ACE	12-Jul-06
S & T	Rail Security Pilot Study Phase 2	12-Jul-06
TSA	Visitor Management System	14-Jul-06
NPPD/US-VISIT	Interim Data Sharing Model for the Automated Biometric Identification System (IDENT)	31-Jul-06
CBP	Western Hemisphere Travel Initiative	11-Aug-06
NPPD/US-VISIT	US VISIT E-Passport	18-Aug-06
TSA	Traveler Identity Verification Program	31-Aug-06
NPPD/US-VISIT	IDENT / Integrated Automated Fingerprint Identification System (IAFIS) Interoperability Project	01-Sep-06
TSA	Registered Traveler (2)	01-Sep-06
FEMA	National Disaster Medical Systems Professional Credentials	13-Oct-06
MANAGEMENT	Homeland Security Presidential Directive (HSPD) 12	17-Oct-06
MANAGEMENT	ePerformance Updated	17-Oct-06
US ICE	Electronic Travel Document	17-Oct-06
USCIS	Background Check Service	31-Oct-06
CBP	Global Online Enrollment System	01-Nov-06
USCG	U.S. Coast Guard (USCG) Mona Pass	01-Nov-06

Component	Name of System	Date Approved
CBP	Automated Targeting System	22-Nov-06
S & T	Disaster Management E-Gov/ Disaster Management Interoperability Services	19-Dec-06
TSA	Transportation Security Administration (TSA) Security Threat Assessment for Airport Badge and Credential Holders	20-Dec-06
TSA	Alien Flight Student Program, addendum	21-Dec-06
TSA	Threat Assessments for Access to Sensitive Security Information for Use in Litigation	28-Dec-06
TSA	Transportation Worker Identification Credential Program	29-Dec-06
NPPD	DHS Center for Faith-based and Community Initiatives	05-Jan-07
USCIS	Integrated Digitization Document Management Program	05-Jan-07
MANAGEMENT	Learning Management System/DHScovery	16-Jan-07
FEMA	eGrants	16-Jan-07
DHS Wide	Redress and Response Record System (Traveler Redress Inquiry Program [TRIP])	17-Jan-07
USCIS	Naturalization Redesign Test Pilot	18-Jan-07
CBP	Western Hemisphere Travel Initiative	23-Jan-07
TSA	Claims Management System	07-Feb-07
FEMA	NFIP Map Service Center	26-Feb-07
DHS Wide	REAL ID Notice of Proposed Rulemaking (NPRM)	01-Mar-07
NPPD/US-VISIT	Inclusion of I-94 Data into the Arrival and Departure Information System (ADIS)	27-Mar-07
NPPD	Chemical Security Assessment Tool	27-Mar-07
USCIS	Biometric Storage System	28-Mar-07
TSA	Tactical Information Sharing System	29-Mar-07

Component	Name of System	Date Approved
USCIS	Verification Information System	02-Apr-07
NPPD	24 x 7 Incident Handling & Response Center	02-Apr-07
MANAGEMENT	Automated Continuing Evaluation System Pilot	09-Apr-07
NPPD/US-VISIT	Automated Identification Management System - disposition of SORN	15-May-07
NPPD/US-VISIT	Enumeration	24-May-07
USCG	MonaPass Web Portal Update	24-May-07
USCIS	Secure Information Management Service Pilot	24-May-07
NPPD	Chemical Security Awareness Training Update	29-May-07
DHS Wide	Contact Lists	18-Jun-07
NPPD	Protected Critical Infrastructure Information Program	20-Jun-07
USCIS	U.S. Citizenship and Immigration Services (USCIS) Enterprise Service Bus	27-Jun-07
USCIS	Enterprise Services Bus- hosted service (Person Centric Query)	28-Jun-07
OPERATIONS	HSIN - COI	28-Jun-07
USCIS	Central Indexing System	28-Jun-07
CBP	Secure Border Initiative-net (SBINet)	20-July-07

14.2. System of Records Notices

Component	Name of System	Date Published in Federal Register
NPPD/US-VISIT	DHS Automated Biometric Identification System	27-Jul-06
TSA	General Legal Records	18-Aug-06
INFRASTRUCTURE	HSPD-12 Personal Identity Verification Management System	11-Sep-06
INFRASTRUCTURE	HSPD-12 Office of Files Security System	11-Sep-06
FEMA	National Disaster Medical System	13-Oct-06
INFRASTRUCTURE	ePerformance	27-Oct-06
CBP	Automated Targeting System	01-Nov-06
USCIS	Background Check System	04-Dec-06
DHS Wide	General Information Technology Access Account Records System	29-Dec-06
USCIS	Alien File (A-File)	16-Jan-07
DHS Wide	DHS Redress and Response Records System	18-Jan-07
USCIS	Biometric Storage System	06-Apr-07
USCIS	Verification Information System	09-Apr-07
NPPD/US-VISIT	Automated Identification Management System - Disposition	25-May-07
USCIS	Background Check System- Adoptions update	04-Jun-07
USCIS	Secure Information Management Service (Pilot)	04-Jun-07
NPPD/US-VISIT	IDENT-Enumeration update	04-Jun-07

Component	Name of System	Date Published in Federal Register
NPPD/US-VISIT	DHS Automated Biometric Identification System	27-Jul-06
TSA	General Legal Records	18-Aug-06
INFRASTRUCTURE	HSPD-12 Personal Identity Verification Management System	11-Sep-06
INFRASTRUCTURE	HSPD-12 Office of Files Security System	11-Sep-06
FEMA	National Disaster Medical System	13-Oct-06
INFRASTRUCTURE	ePerformance	27-Oct-06
CBP	Automated Targeting System	01-Nov-06
USCIS	Background Check System	04-Dec-06
DHS Wide	General Information Technology Access Account Records System	29-Dec-06
USCIS	Alien File (A-File)	16-Jan-07
DHS Wide	DHS Redress and Response Records System	18-Jan-07
USCIS	Biometric Storage System	06-Apr-07
USCIS	Verification Information System	09-Apr-07
NPPD/US-VISIT	Automated Identification Management System - Disposition	25-May-07
USCIS	Background Check System- Adoptions update	04-Jun-07
USCIS	Secure Information Management Service (Pilot)	04-Jun-07
NPPD/US-VISIT	IDENT-Enumeration update	04-Jun-07