Annual Report

Privacy Office Annual Report to Congress

July 2007 – July 2008

Homeland Security

Privacy Office
Annual Report to Congress
July 2007 – July 2008

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

July 2008

LETTER FROM THE CHIEF PRIVACY OFFICER

I am pleased to present the fourth Annual Report issued by the Department of Homeland Security (DHS) Privacy Office. This report covers the period of July 2007 through July 2008. This and all previous Annual Reports are posted on the DHS Privacy Office website at www.dhs.gov/privacy.

The Department and the Privacy Office have been operational for over five years. As of the conclusion of this reporting period, I have had the privilege of serving in the Privacy Office for two years and have overseen the release of three annual reports. This was another year of noteworthy and continued growth and progress for the DHS Privacy Office. As I mentioned in the previous Annual report, we saw this Annual Reporting cycle as "a period of significant opportunities for the Department to expand the presence of Privacy Officers and Privacy Points of Contact (PPOCs) within DHS operational components." And it was. This year, we doubled the Federal employees within the office, and, as planned, expanded the network of component Privacy Officers and PPOCs. Expanding the pool of knowledgeable privacy personnel throughout the Department continues to increase the efficiency with which we can fulfill the DHS Privacy Office's statutory requirements to meet the mission of the office, and support the Department's mission.

The Privacy Office also issued a number of critical written policy documents and guidance. In doing so, my colleagues and I made great progress in formalizing privacy processes and operations to ensure we effectively support the Department. During this reporting period, we updated critical compliance guidance, such as the System of Records Notice (SORN) Guidance; issued new guidance, such as the Privacy Act (e)(3) Statements guidance and *Privacy Technology Implementation Guide (PTIG)*; and implemented privacy guidance that was new during the previous reporting period, such as the *DHS Privacy Incident Response Plan*. Additionally, we made great strides in addressing new requirements, such as *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-73). We continue to examine our requirements as a Department and identify additional opportunities to develop meaningful privacy guidance.

During this reporting period, we addressed several key issues. Our Privacy Compliance Group initiated a Legacy SORN Update project to review and update legacy SORNs that remained operative under a savings provision of the Homeland Security Act and were carried over from the Department's creation. In order to coordinate and expedite the review effort, we dedicated full-time resources to this effort. Additionally, our Disclosure and Freedom of

Information practice made significant progress in reducing the backlog of *Freedom of Information Act* (FOIA) requests by developing and executing a strategy to address the backlog. The success to date of the Legacy SORN Update and FOIA teams would not be possible without the collaboration and support of our privacy colleagues and their leadership throughout the Department.

In addition to continuing to work closely with our DHS colleagues, the DHS Privacy Office continues to focus on outreach with the Federal, State, local, and international communities. We continued building on our efforts with the Department of Justice (DOJ) and the Project Manager of the Information Sharing Environment to support State and local fusion centers. We expanded our own knowledge and continued building our outreach presence by speaking at and/or attending over 50 events regarding relevant privacy issues in both the U.S. and internationally.

As I reflect on the past two years as Chief Privacy Officer, I am proud of the achievements of my privacy colleagues throughout DHS. I have had the pleasure of working with the best and brightest individuals in the Federal privacy community. Together we fostered a culture of privacy awareness throughout the Department and the Federal Government. We build upon that foundation every day and I look forward to seeing more great leadership from this office in the years to come.

Thank you for your continued support of the DHS Privacy Office.

Hugo Teufel III

Chief Privacy and Freedom of Information Act Officer
U.S. Department of Homeland Security

TABLE OF CONTENTS

1. Overview of DHS Privacy Office Responsibilities and Activities

The mission of the DHS Privacy Office (the "Privacy Office" or "Office") is founded upon the responsibilities set forth in Section 222 of the *Homeland Security Act of 2002* ("Homeland Security Act")[Public Law 107-296; 6 U.S.C. 142], as amended. The DHS Chief Privacy Officer's responsibilities include:

- Assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information;
- 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* ("Privacy Act") [5 U.S.C. § 552a];
- Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal government;
- 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;
- 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
- 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.

In addition to the responsibilities described above, 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* ("9/11 Commission Act") [Public Law 110-53], passed on August 3, 2007. Section 802 of the Act codified authority of the Chief Privacy Officer to investigate and or report on DHS programs and operations with respect to privacy, while creating additional obligations to coordinate investigations of violations or abuse related to privacy with the DHS Office of Inspector General (OIG). This investigatory authority now expressly includes: access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to privacy within the programs and operations; the power to issue subpoenas to any person other than a Federal agency, with the approval of the Secretary; and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under Section 222 of the Homeland Security Act. These new responsibilities are described in detail in Section 4.

The Privacy Office has other general statutory and policy-based responsibilities, including implementation of Section 208 of the *E-Government Act of 2002* ("E-Government Act") [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).[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* (FOIA), as amended [5 U.S.C. § 552], and requests made under the Privacy Act.

The Privacy Office's privacy compliance policies and procedures are based on a set of eight fair information practice principles (FIPPs) that are rooted in the tenets of the Privacy Act and govern the appropriate use of personally identifiable information (PII). DHS uses the FIPPs 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 FIPPs is described below:

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

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

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

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

[1] See Section 2e, Guideline 5 of the Presidential Memorandum issued December 16, 2005.

- Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.
- Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

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

The Office continues to grow along with the increasing responsibilities and coordination required to support its mission and the mission of the Department. The Office doubled in size from Fiscal Year (FY) 2007 to FY08, increasing from 16 positions to 32, with a budget increase of almost $1 million, from $4.55 million to $5.5 million. As part of this expansion, the Privacy Office added the following positions:

- Privacy compliance specialists (5)
- FOIA Program Specialists (5)
- Administrative Specialists (2)

As of July 2008, the Office currently has 24 full-time equivalents, one DHS Fellow, and seven contractors. The Office is in the process of bringing on board a Director of Privacy Incidents and Inquiries, Associate Director of Privacy Technology and Intelligence, Associate Director of Privacy Policy and Education, Attorney-Advisor, one FOIA Administrative Specialist and three FOIA Program Specialists. Additionally, the Office is recruiting for a Privacy Analyst and Senior Attorney Advisor. The Privacy Office will continue to promote growth in component privacy programs as a critical means of addressing privacy requirements throughout the Department. Component support is discussed in detail in Section 2.8.

The Privacy Office also developed its managers and its capacity for continuity of operations. The Office's two senior deputies, the Deputy Chief Privacy Officer and Deputy Freedom of Information Act and Disclosure Officer earned certificates in management training courses. These two senior career positions will enable the Office to continue implementing Privacy Office responsibilities in the absence of an appointed Chief Privacy Officer. Regarding continuity of operations, the Office established a formal succession plan and senior staff in the

Office participated in a two day off-site emergency planning exercise. In preparation for the upcoming change of administration, the deputies have also participated in transition meetings with other senior career staff throughout the Department.

2. Compliance

The work of the Privacy Compliance Group of the DHS Privacy Office is the engine that drives privacy implementation at the Department. The Compliance Group supervises the completion and approval of all Privacy Threshold Analyses (PTAs), PIAs, and SORNs throughout DHS. The below sections report total counts of completed PTAs, PIAs, and SORNs. These numbers represent totals completed by fiscal year through July 1, 2008. Additionally, the Privacy Compliance Group conducts privacy reviews of DHS systems and programs as appropriate.

As part of the compliance process, the Privacy Compliance Group works with component Privacy Officers, PPOCs, program managers, and system owners at Headquarters and all DHS components to ensure sound privacy practices and controls are integrated into the Department's operations. To promote privacy compliance within the Department, the Compliance Group has published official Department guidance regarding the requirements and content of the following:

- PTAs (updated previous guidance);
- PIAs (updated previous guidance);
- SORNs; and
- Privacy Act (e)(3) Statements.

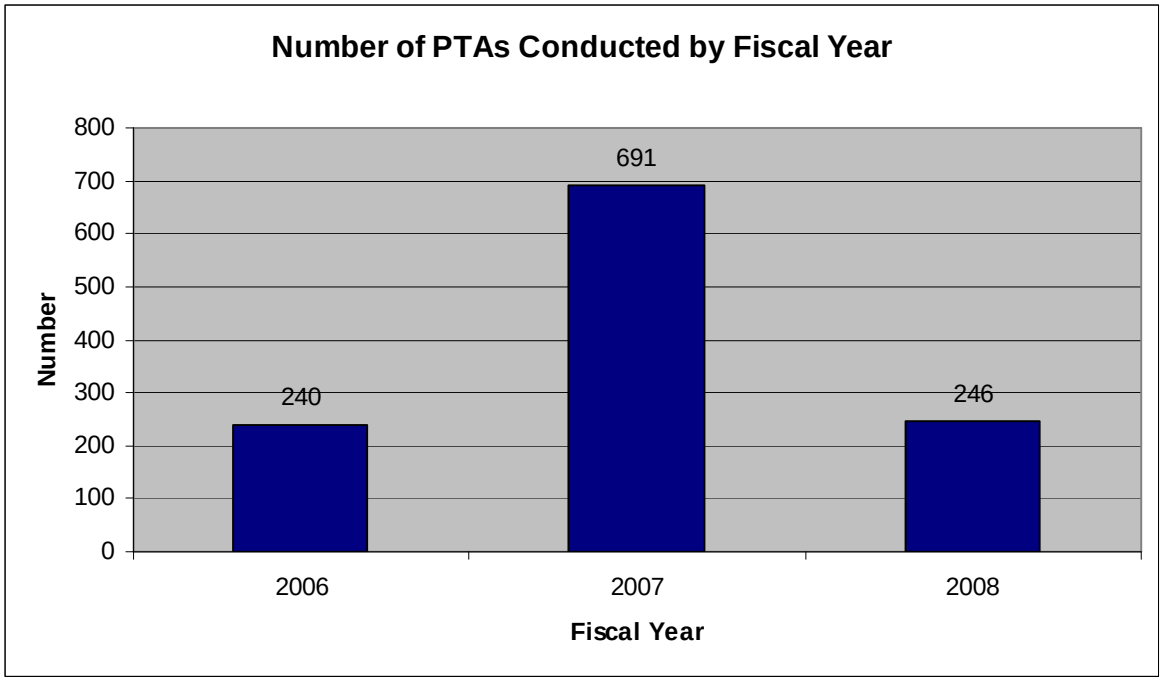
A critical project for the Privacy Compliance Group during this reporting period was updating and revising operational components' SORNs to reflect information oversight and integration within DHS. All DHS components are actively working to complete the project by winter 2008.

Each year, the Compliance Group reviews all Office of Management and Budget (OMB) Exhibit 300 budget submissions to determine whether new and existing programs have appropriately addressed privacy and have completed the required documentation. During the FY09 budget process ending September 2007, the Privacy Compliance Group failed five investments due to insufficient privacy protections and privacy documentation. The Privacy Compliance Group is now closely coordinating with the affected programs to embed privacy into the developmental and operational processes to provide appropriate protective measures.

2.1. Privacy Threshold Analyses

Although PIAs are commonly performed throughout the Federal government, the DHS Privacy Office developed the PTA in November 2005 as part of the Certification and Accreditation

(C&A) process[2] for systematically assessing the privacy of information technology (IT) systems. DHS completed the first PTAs beginning in early 2006 and made a major push to complete PTAs for all systems throughout 2007 and into 2008. PTAs on all existing systems were completed in 2007. DHS now performs PTAs on all operational systems and continues to use them as an important tool when changes are made and new systems are developed. The PTA was specifically designed to identify systems in the DHS information system inventory collecting or using PII, denoting which systems require a PIA, and which need a SORN. The DHS Privacy Office has further refined the PTA over the past three years, and it is now a key aspect of the privacy compliance process. The most recent update to the PTA template identifies systems that permit data extracts and remote access, as required by OMB M-06-16[3] and OMB M-07-16[4], and is used to designate privacy sensitive systems.



The PTA outlines general information about a system, including the year the system was developed/modified, description of the system, what PII the system collects or uses, if any, and from whom. The Privacy Compliance Group reviews the PTA, and then engages in a detailed dialogue with the program manager, information security officer, or PPOC, as necessary. The Director of Privacy Compliance determines whether a PIA or SORN is required based on the PTA. If the PTA review demonstrates that a full PIA is required, the program must complete the

[2] The system C&A process is required by Federal Information Security Management Act of 2002 [Public Law 107-347] and is overseen by the DHS Chief Information Security Officer (CISO).

[3] Office of Management and Budget (OMB) Memorandum 06-16, *Protection of Sensitive Agency Information.*

[4] OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

PIA using the DHS *Privacy Impact Assessments, Official Guidance* ("PIA Guidance") and return the completed PIA to the DHS 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 C&A inventory, but also to formally document other decisions made by a program affecting privacy. For example, the PTA is now used to document and track all systems collecting Social Security Numbers (SSNs) from the public. The two examples below describe scenarios for PTA and PIA use.

Example One:

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.), 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.

Example Two:

DHS published a DHS-wide PIA covering contact lists. When a program is notified they may 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 an existing PIA.

A template for the PTA is available on the DHS Privacy Office website under the "Privacy Office Official Guidance" webpage.[5] From July 1, 2007, through July 1, 2008, the DHS Privacy Office reviewed and validated approximately 315 PTAs.

2.2. Privacy Impact Assessments

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 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) to conduct PIAs for proposed rulemakings of the Department.

[5] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf

The PIA is a crucial mechanism used by the Chief Privacy Officer to fulfill these statutory mandates and to "operationalize" privacy at the Department. First, a PIA is a deliberative document in that it forces a program to consider privacy throughout its development lifecycle.[6] Second, a PIA provides the public greater transparency of government operations, often more so than the SORN. Third, the E-Government Act and the Homeland Security Act provide for PIAs. Fourth, in some cases Congress has tied funding to completion of a PIA.

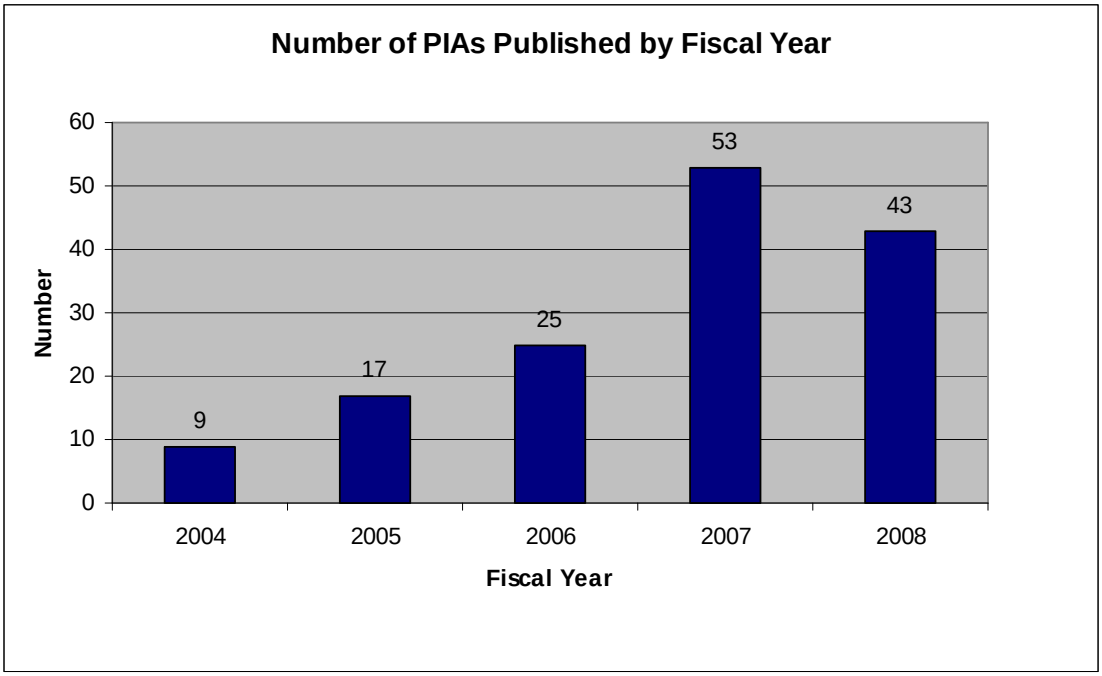
PIAs are a central component of the Department's privacy compliance efforts. By conducting PIAs, DHS demonstrates its commitment to implementing privacy practices and controls early in the development process of the Department's programs and systems; thus upholding the Department's commitment to maintaining 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.

PIAs demonstrate that system owners and developers consciously incorporate 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 March of 2008 the DHS Privacy Office published a PIA on the Office of the Chief Human Capital Officer's e-Recruitment system which manages the recruitment and hiring of individuals at DHS. The DHS Privacy Office also worked with the United States Citizenship and Immigration Services (USCIS) on PIAs for its Verification Division, which is charged with providing immigration status verification for benefits determinations and verification of employment authorization for newly hired employees.

The DHS Privacy Office coordinates the completion of PIAs for the Department and all components. The Chief Privacy Officer approves all Department and component PIAs. Summary abstracts of completed PIAs are posted on the DHS Privacy Office website and a compendium of posted abstracts is published in the Federal Register (FR) on a monthly basis.[7]

[6] The term "development lifecycle" refers to the phases of program or system development from conception, design, development, testing, and deployment, to retirement.

[7] PIAs are posted at the following link on the DHS Privacy Office website: www.dhs.gov/privacy, then follow links to Privacy Impact Assessments.



Between July 1, 2007, and June 30, 2008, the DHS Privacy Office approved and published 53 PIAs. The DHS Privacy Office also reviewed and approved five PIAs for National Security Systems for the Office of Intelligence and Analysis (I&A). These are conducted to integrate privacy protections into I&A programs and provide assistance and oversight to Congress, OIG, and the DHS Privacy Office prior to deployment. Given the sensitivity of the systems, however, PIAs for national security systems are not published. Appendix A provides a list of all approved and published PIAs during the reporting period.

2.3. PIA Guidance

As privacy compliance at DHS has matured, so have the content and procedures for conducting a PIA. In 2005, the DHS Privacy Office first published its PIA Guidance and the associated PIA template for use by the Department and component staff responsible for drafting PIAs for their programs and systems. Updated in July of 2006 and May 2007, the Department's PIA Guidance has been used as a model by other Federal agencies on how to approach and conduct PIAs.

The PIA Guidance is designed to capture the various requirements of the E-Government Act and Department policy. The PIA guidance requires that PIAs address general areas, such as scope of the information collected, uses, information security, and information sharing, to name a few, and also presents specific questions on the use of commercial data, data analysis tools, and specific compliance with the relevant system's SORN. Furthermore, each section of the PIA concludes with an analysis section designed to outline any privacy risks presented by the section's questions, and discuss any strategies or practices used to mitigate those risks. It is these

analysis sections which reinforce critical thinking about the program and privacy during the early stages of program development.

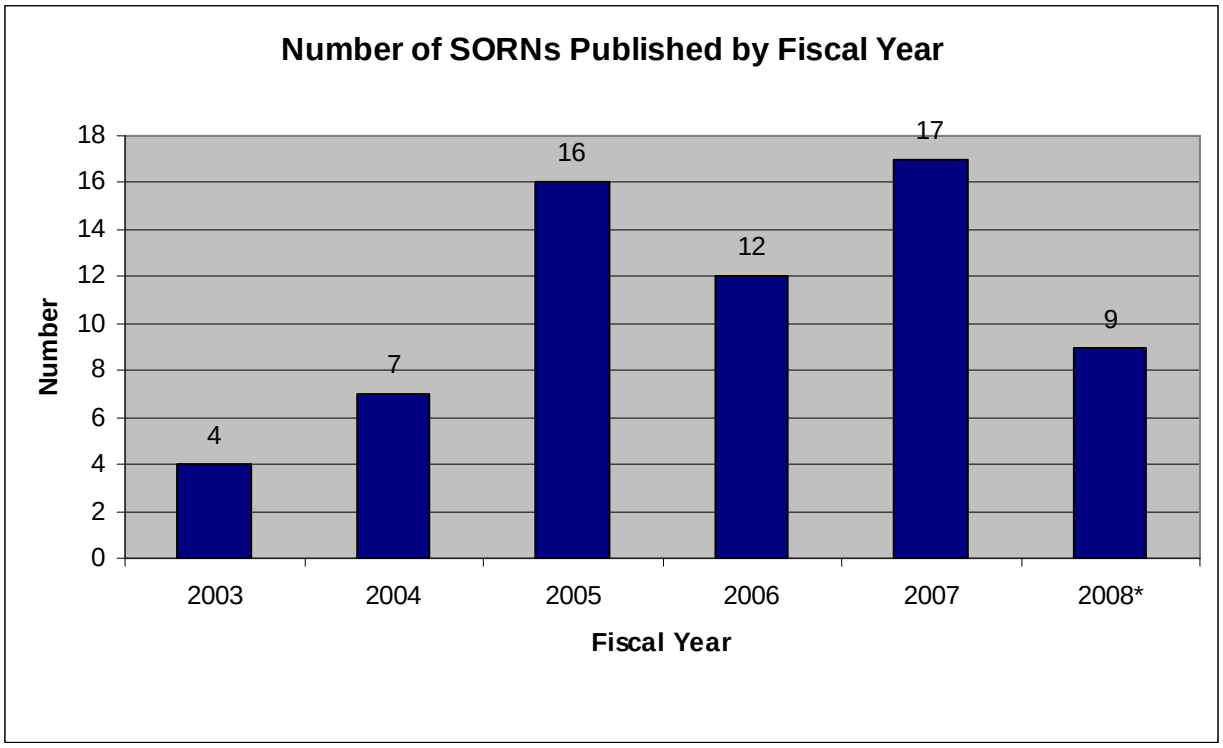
As an example, United States Coast Guard (USCG) replaced an old system of records/IT system (Joint Maritime Information Element [JMIE] Support System [JSS]) with the modernized and integrated Maritime Awareness Global Network (MAGNET). MAGNET's aggregation and correlation of maritime data allows USCG to easier understand and interpret security maritime data. The PIA identified certain privacy risks, including the large amount of information collected and the potential for unauthorized disclosure or misuse of this information. USCG recognized that although a large amount of data is collected and used, a number of protections were in place. First, the USCG already possessed such information lawfully, and the information was statutorily and mission-limited to the USCG's maritime sector authority. Second, PII within MAGNET is specifically tagged to ensure that users understand that PII is to be handled with care and in accordance with relevant regulations related to law enforcement and intelligence activities. Third, all use of information and disclosure from the system is audited regularly. Completion of the MAGNET PIA was a complex endeavor and required significant cooperation and dialogue between the DHS Privacy Office and USCG.

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

2.4. System of Records Notices

The Privacy Act requires Federal agencies to publish a SORN in the *Federal Register* when PII is maintained by a Federal agency in a system of records and the information is retrieved by a personal identifier. The SORN describes, among other things, the purpose of the collection, information sharing, categories of records and individuals covered, record retention and destruction, and how records are retrieved within the system.

Section 222(2) of the Homeland Security Act specifically authorizes the Chief Privacy Officer to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with the fair information practices as set out in the Privacy Act." Those principles are detailed in the SORN Guidance issued in May 2008, as well as in the PIA Guidance for the Department.



From June 30, 2007, to July 1, 2008, the Department published or updated 12 System of Records Notices. DHS is also in the process of reviewing and updating its legacy agency SORNs. These SORNs provide significant notice and transparency of Department operations and give the public a meaningful opportunity to participate in the rulemaking process.

For example, the DHS Privacy Office worked with Customs and Border Protection (CBP) to issue the Advance Passenger Information System (APIS) SORN, PIA, and Notice of Proposed Rule Making (NPRM). Previously, some traveler information had been stored in another system of records within CBP. Publishing the APIS SORN permits the traveling public greater access to individual information, and a more complete understanding of how and where information pertaining to them is collected and maintained.

Similarly, the DHS Privacy Office worked with the Transportation Security Administration's (TSA) Secure Flight program to publish a SORN and NPRM detailing the changes made to Secure Flight based in part on comments received from the public on previously issued Secure Flight documents. The comment process provides for public participation in the implementation of DHS programs which directly affect them.

2.4.1. Legacy SORN Project

As part of the Department's effort to streamline and consolidate its legacy Privacy Act systems of records, the DHS Privacy Office is reviewing and updating its legacy SORNs. These SORNs were carried over from legacy agencies with the creation of the Department in January

2003. And while a savings provision within the Homeland Security Act preserves the coverage of these legacy SORNs, the Chief Privacy Officer is committed to the effort to update them.

In September 2007, the Chief Privacy Officer increased resources to enable the DHS Privacy Office to move the review forward in a more coordinated and expeditious fashion. Through this review, the DHS Privacy Office and components have had the opportunity to:

- Review and identify obsolete and out-of-date SORNs;
- Develop a consistent privacy approach for Department records;
- Update SORNs to reflect the mission of the Department; and
- Increase transparency to the public and Department employees about the use of PII.

The SORN review effort includes four phases: 1) legacy SORNs to be retired under Federal Government-wide SORNs; 2) legacy SORNs to be retired under existing DHS-wide SORNs; 3) legacy SORNs to be retired under newly created DHS-wide SORNs; and 4) legacy SORNs to be reissued as DHS-component specific SORNs.

Addressing these legacy SORNs and issuing necessary updates directly supports Secretary Chertoff's priority goal # 5: *Strengthen and Unify DHS Operations and Management* by utilizing the already established resources in the PPOC network, and communication with component Privacy Officers, program managers, and system owners to streamline and consolidate legacy SORNs. Additionally, this effort supports the Department's objective to become "One-DHS" by using the resources of every DHS component to streamline processes and ensure that DHS remains in compliance with the Privacy Act. It is of utmost importance that the Department continues to uphold public trust in daily operations to secure the homeland and reconfirms that the disclosure of the public's personal information is restricted to the appropriate routine uses outlined in the SORNs at all times.

2.4.2. SORN Guidance

In May of 2008, the DHS Privacy Office published *System of Records Notices: Official Guidance*, the Department's guidance to drafting System of Records Notices as required by the Privacy Act. Much like the PIA Guidance, the SORN Guidance is designed to enable SORN drafters to properly draft each section of the notice.

The SORN Guidance and accompanying template cover the requirements for identifying a system of records, the elements of a SORN, and publishing a SORN. The Guidance briefly discusses exemptions to the Privacy Act as addressed in NPRMs and Final Rules. The new guidance replaces the SORN guidance previously issued in February 2004 and augments, for DHS' purposes, guidance previously issued by the Office of Management and Budget, specifically *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975, and *Circular A-130* including *Appendix I*, November 28, 2000.

2.5. FISMA Privacy Reporting

Privacy and information security are closely linked, and strong practices in one area typically supports the other. In fact, security is one of the FIPPs. To that end, the Privacy Office works closely with the Chief Information Security Officer (CISO) to monitor the privacy requirements under the Federal Information Security Management Act (FISMA)[8]. On a quarterly and annual basis, DHS reports to OMB its progress in conducting PIAs and issuing SORNs for IT systems that are required to go through the FISMA C&A. At the end of the FY07 reporting period, October 1, 2007, DHS had conducted PIAs on 26% of the IT systems that required PIAs and 66% of the IT systems were covered by a SORN. By July 1, 2008, DHS had improved its FISMA privacy numbers to 40% for PIAs and 84% for SORNs. The components with the best scores include TSA and the National Protection and Programs Directorate's (NPPD) component program, U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). The components with scores significantly below the average for PIAs were USCIS, United States Immigration and Customs Enforcement (ICE), Federal Emergency Management Agency (FEMA), and USCG. Components with scores significantly below the average for SORNs were FEMA and ICE. The Privacy Office anticipates improvement of the USCIS and ICE scores due to the newly appointed Privacy Officers who report to the heads of their components.

2.6. Privacy Act Statement Guidance

In April, the DHS Privacy Office released the *Privacy Act Statements Guidance* ("(e)(3) Statements") pursuant to the Privacy Act of 1974, 5 U.S.C. §552a (e)(3), as amended.[9] The Privacy Act requires agencies to provide a Privacy Act Statement whenever individuals are asked to provide personal information. The Privacy Act Statement must state the authority to collect the information, the purpose of the collection, the routine uses and disclosure of the information, and whether the collection is mandatory or voluntary. These statements are a fundamental means of informing the public about the information the government is collecting from them.

2.7. OMB Exhibit 300s

All major programs are reviewed on an annual basis, prior to submission to OMB for inclusion in the President's annual budget. Submissions must demonstrate, among other things, that the agency has properly addressed privacy. The DHS Privacy Office plays a substantial role in the review of the OMB Exhibit 300s prior to submission to OMB. Also referred to as the "OMB 300" process, the 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

[8] Public Law 107-347.

[9] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_e3.pdf

review of each investment portfolio includes an examination of the privacy protections implemented within the individual systems associated with that investment, and whether the protections are documented in a PIA or SORN. The DHS 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 DHS 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 FY09 budget process, the Privacy Compliance group reviewed investments and associated systems. To receive a passing score, submissions must include the appropriate privacy documentation or the DHS Privacy Office must determine the investment does not require privacy documentation. Conversely, the Office rejected five investments because of insufficient privacy protections and privacy documentation. The Privacy Compliance group has worked with each of the five programs to ensure that the appropriate protections and privacy documentation are in place. As of July 1, 2008, three of the rejected investments were subsequently revised and recommended for approval by the DHS Privacy Office and DHS to OMB. The Privacy Office continues to work with the other two programs to ensure they have appropriate privacy protections.

The DHS Privacy Office is currently in the middle of the FY10 review process. The final approval and rejection numbers will be provided to OMB once the budget submissions are due, and will be reported in the DHS Privacy Office Annual Report for next year.

2.8. DHS Sensitive Systems Policy Directive 4300A

The Office of the CISO has issued DHS Sensitive Systems Policy Directive 4300A and its accompanying handbook as the foundation for IT security of sensitive systems at the Department. This policy document also supports the Department's privacy requirements. During the past year, the DHS Privacy Office reviewed and updated sections of 4300A that affect privacy policy at DHS, including sections regarding roles and responsibilities and management policies.

In addition to providing updates to 4300A, the DHS Privacy Office, in coordination with the CISO, developed Attachment S to 4300A. This new attachment formally implements OMB Memorandum 06-16 guidance for protecting sensitive agency information. Attachment S, which is based on the National Institute of Standards Technology (NIST) SP 800-53A checklist for the protection of remote information, designates six requirements for protecting Privacy Sensitive Systems that permit remote access or allow for the removal of sensitive information outside of internal agency controls.

One of the requirements for protecting privacy sensitive systems is the process of authorizing, approving, and tracking PII extracts from DHS systems. In response to this requirement and the need for standard operating procedures (SOPs) to supplement Attachment S, the DHS Privacy Office has established a Data Extracts Working Group. The group, made up of privacy personnel from various components, is in the process of developing a set of SOPs to establish uniform practices throughout the Department for authorizing, approving, and tracking data extracts.

2.9. Component Privacy Officers and Privacy Points of Contact

Establishing and increasing the number of well-trained Privacy Officers at the component level helps build privacy into new programs at the beginning of the development process and existing programs as they are updated. Component Privacy Officers and PPOCs ensure programs in their component agencies identify privacy issues and work with the DHS Privacy Office to address them. The DHS Privacy Office works closely with component Privacy Officers and PPOCs to implement privacy policies and practices across the Department.

The designation of Privacy Officers within operational and department-level components significantly involved with PII is a high priority for the DHS Privacy Office. While the DHS Privacy Office retains expertise in all types of privacy issues, the overall mission of the DHS Privacy Office is increasingly demanding. The component Privacy Officers report to the component head, and coordinate with the DHS Privacy Office for privacy compliance and Department-wide initiatives. Prior to this reporting period, TSA and US-VISIT had dedicated Privacy Officers.[10]

In November 2007, the Secretary, at the Chief Privacy Officer's recommendation, signed a memorandum directing the operational and Department-level components to appoint full-time Privacy Officers as senior staff reporting to component heads. The components required to designate Privacy Officers are CBP, USCIS, FEMA, ICE, I&A, and the Science and Technology Directorate (S&T). Designating a Privacy Officer elevates privacy responsibilities to a more effective level of authority and visibility within each component. The Secretary's memorandum designating these Privacy Officers includes a defined set of responsibilities for all Privacy Officers at the Department. The table that follows shows the status of each component's progress in designating a Privacy Officer.

[10] NPPD's National Cyber Security Division (NCSD) has also had a Privacy Officer in the past, but did not have one during this reporting period.

Component	Privacy Officer Status	Notes
FEMA	●	Privacy Officer designated
ICE	●	Privacy Officer designated
TSA	●	Privacy Officer designated prior to the Secretary's memorandum
USCIS	●	Privacy Officer designated
S&T	●[11]	Privacy Officer designated, however, position is currently filled by contractor
CBP	●[12]	Privacy Officer not designated
I&A	●[13]	Privacy Officer not designated

In addition to the component requirements above, several major programs chose to designate Privacy Officers to better support privacy efforts, including the USCIS' E-Verify program, TSA's Secure Flight program and the NPPD US-VISIT program. The Privacy Office also sees a need for a Privacy Officer in NPPD's National Cyber Security Division (NCSD) and the newly created National Cyber Security Center. CBP, I&A, and U.S. Secret Service (USSS) have PPOCs who work on a daily basis with the DHS Privacy Office to handle component privacy-related matters, including processing programs and systems through the privacy compliance operation, assisting with drafting PTAs, PIAs, and SORNs, and responding to privacy incidents.

[11] The S&T contractor has assumed all of the Privacy Officer's responsibilities.

[12] CBP has advised that two individuals within CBP, the responsible Senior Executive and the Privacy Lead, have assumed some of the Privacy Officer responsibilities.

[13] Subsequent to this reporting period, I&A has begun actively developing its privacy program, which will include identification of a privacy officer. Currently, I&A has a full-time contractor who has assumed some of the Privacy Officer's responsibilities.

The chart below identifies the grade-level of component Privacy Officers or privacy leads as well as the number of PPOCs and other component privacy positions.[14]

Components	Grade-level of Privacy Officer/Privacy Lead	Additional Full-Time Privacy Positions
CBP	GS-15	11
CIS	GS-15	1
FEMA	GS-15	2
I&A	GS-15[15]	0
ICE	GS-15	1[16]
S&T	GS-15[17]	2
TSA	GS-15[18]	3
Programs		
E-Verify	GS-15	5[19]
US-VISIT	GS-15	7[20]

The DHS Privacy Office hosts a monthly Privacy Compliance Meeting for the all of the component Privacy Officers and PPOCs. The purpose of these meetings is to foster two-way communication between the DHS Privacy Office and the broader DHS privacy community. Discussions typically revolve around important DHS Privacy Office initiatives and issues, as well as sharing experiences and advice throughout the DHS privacy community. These meetings are also used as an opportunity to host external privacy colleagues. For example, the DHS Privacy Office hosted the Social Security Administration's Executive Director, Office of Public Disclosure, at the November 2007 Department-wide Privacy Compliance Meeting.

[14] This category includes individuals in addition to the component Privacy Officer or privacy lead. These resources may include dedicated Federal employees and contractors.

[15] The I&A Privacy Officer role is currently filled by a contractor; however, the position is a GS-15 level position.

[16] ICE will have an additional privacy resource beginning in October 2008.

[17] The S&T Privacy Officer role is currently filled by a contractor; however, the position is a GS-15 level position.

[18] TSA is on a pay band system. The Privacy Officer is at pay band L, which is equivalent to a GS-15 or higher.

[19] E-Verify currently has five vacancies in addition to the current resources.

[20] US-VISIT currently has one vacancy in addition to the current resources.

The appointment of component Privacy Officers is a significant step towards strengthening privacy protections at the Department. Notwithstanding, a few components have not yet complied with the Secretary's request. In order to continue increasing the effectiveness of the DHS Privacy Office and building privacy into all DHS programs and systems, the Department will need to continue to expand the network of Privacy Officers and PPOCs. Increasing the number of component Privacy Officers and PPOCs would support better privacy implementation throughout the development and implementation lifecycle of a program. In turn, the DHS Privacy Office could then 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.

The long-term goal of the DHS 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 Officer level, and then have the DHS Privacy Office conduct the final review to approve the privacy documentation, with minimal reworking of the documents by the Privacy Office. In components with dedicated Privacy Officers, this is the case.

3. Component Privacy Programs and Initiatives

Component Privacy Programs and Initiatives continue to expand, both in the number of dedicated privacy personnel and resources, and the number of initiatives they support. The DHS Privacy Office continues to work with component Privacy Officers and PPOCs on these important matters. The following sections discuss some of the high-profile privacy activities for DHS during the reporting period, including USCIS, ICE, S&T, TSA, USCG, and US-VISIT.

3.1. U.S. Citizenship and Immigration Services

USCIS established a formal privacy program and hired its first Privacy Officer in November 2007 to provide full-time support for privacy matters within the component. On July 9, 2008, USCIS took this one step further and established the USCIS Office of Privacy, formally appointing the USCIS Privacy Officer and a Deputy Privacy Officer.

The USCIS Office of Privacy is responsible for the following activities:

- Developing privacy policy;
- Ensuring compliance with applicable privacy mandates in coordination with USCIS program offices and the DHS Privacy Office;
- Conducting training for employees and contractors on privacy laws, regulations and policy; and
- Providing advice and technical assistance to program and system managers in the development of documentation that meets privacy compliance requirements.

The highlights of key accomplishments for USCIS privacy activities during this report period include the following:

- In coordination with the DHS Privacy Office, assessed and re-established PTAs on over 100 existing USCIS IT systems using the new 2007 template.
- Collaborated with USCIS program and system managers to develop new or amended PIAs and SORNs.
- Issued a series of memoranda and other guidance to increase awareness and enhance USCIS employees' knowledge and understanding of Federal privacy laws, statutes, regulations, and policy.

Additionally, the Privacy Office worked with USCIS to publish a PIA for the UKvisas Project. Under the UKvisas project, officials from the UK and DHS agreed that individuals who are physically located in the United States (US) may provide the requisite biometrics and limited biographical information at USCIS Application Support Centers (ASCs) for forward transfer to the UK in support of the adjudication of applications for visas to visit the UK. US VISIT later issued privacy documentation on the complete implementation of this program.

Looking ahead, USCIS will focus privacy efforts on ensuring that all IT systems are compliant with their privacy documentation by December 30, 2008; hiring additional staff in the Office of Privacy in anticipation of increasing workload; developing and implementing a comprehensive privacy training program for USCIS employees and contractors by September 30, 2008; and hosting "USCIS Privacy Week" in Spring 2009.

3.2. U.S. Customs and Border Protection

Between July, 2007, and the end of June, 2008, CBP and the Privacy Office collaborated on the issuance of three SORNs, three NPRMs relating to exemptions for those SORNs, and six PIAs. Together these documents enhanced DHS's and CBP's border security efforts by improving privacy compliance, transparency, and access to information for the traveling public, and ensuring broad coverage for CBP's expanding ability to identify, contemporaneously and in advance, persons seeking to travel to and be admitted into the United States. These privacy compliance documents serve a critical role in building public trust and confidence in CBP's efforts to prevent terrorists and terrorist weapons from entering the United States, while facilitating legitimate travel and trade. Examples of these documents are noted in sections 2.4, 6.2, and 8.1.1 of this report.

Of particular interest was the PIA issued on July 20, 2007, for the Secure Border Initiative-net. This was an innovative PIA in support of a demonstration project for technology supporting the "virtual fence" along the Southern border. The SBInet PIA employed a unique format to explore the potential privacy implications of CBP's use of enhance video surveillance of a test site along the Arizona—Mexico border.

CBP continues to work actively with the Privacy Office to reissue and update the legacy SORNs of its predecessor agencies, as well as to support the compliance of new initiatives being pursued to enhance border security.

3.3. U.S. Immigration and Customs Enforcement

ICE established a Privacy Office and hired its first full-time Privacy Officer in April 2008. The immediate goals for the new ICE Privacy Office include addressing all legacy SORNs by the end of calendar year 2008 as part of the DHS Privacy Office Legacy SORN project, ensuring PIAs are conducted on all appropriate IT systems in compliance with the e-Government Act of 2002, developing enhanced procedures for privacy incident notification and remediation, and developing contract language to enhance the privacy and security of PII held by contractors.

Additionally, the Privacy Office worked closely with ICE to publish a PIA, SORN, NPRM, and Final Rule for the ICE Pattern Analysis and Information Collection (ICEPIC) toolset. ICEPIC assists ICE law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations that are indicative of violations of the customs and immigration laws as well as possible terrorist threats and plots. The Privacy Office worked closely with ICE to ensure that appropriate privacy measures were in place. All ICEPIC activity is predicated on ongoing law enforcement investigations, and all ICEPIC searches are evaluated by a human analyst to ensure relevance and significance. ICEPIC also has strict auditing and access controls over the use and access to information.

3.4. Science and Technology Directorate

S&T is the primary research and development arm of DHS. S&T's mission is to protect the homeland by providing Federal, state, local, tribal, and territorial officials with state-of-the-art technology and other resources. S&T works in partnership with the private sector, the academic community, and other government agencies to encourage innovation in homeland security research and technology development.

Starting this year, S&T dedicated a full-time contractor position to focus exclusively on privacy issues related to the Department's science and technology research. S&T's increased dedication to privacy protection policies and practices expanded the breadth and depth of the collaboration between S&T and the DHS Privacy Office to address the unique challenges of integrating privacy protections into the new technologies and capabilities S&T creates for the Department. Through the active collaboration of S&T and the Privacy Office on new privacy and technology issues, the Department can offer its components expanded means to improve its programs' abilities to fulfill DHS's complex responsibilities to protect our nation and its defining social values.

3.4.1. S&T Privacy Compliance Data Call and Documentation

S&T conducted a comprehensive data call of all systems, projects, and initiatives within the Directorate to locate all PII collected, stored, maintained, or generated by S&T. S&T drafted and submitted PTAs, PIAs, and SORNs to document each system, project, or initiative identified in the data call.

3.4.2. S&T Training and Outreach

The S&T PPOC initiated the following training and outreach activities throughout the Directorate:

- Conducted outreach briefings for the Innovation Division, the Human Factors Division, the Explosives Division, the Transportation Security Laboratory, the Office of University Programs, the People Screening Capstone Integrated Product Team, and Program Managers overseeing privacy-sensitive research efforts.
- Distributed S&T-wide emails providing guidance on the identification and proper handling of electronic files and paper documents containing PII.
- Planned and executed the Department's first ever "Privacy Day" during which S&T accomplished the following objectives:
  - Conducted annual privacy training for more than 1,000 S&T employees and contractors;
  - Held a question-and-answer session for Program Managers with the DHS Privacy Office;
  - Audited portable devices to ensure compliance with DHS policy regarding the storage of PII; and
  - Conducted a "file clean-up" to ensure all paper and electronic files containing PII were properly protected and to appropriately dispose of PII that no longer needed to be maintained.
- Conducted two site visits to the Transportation Security Laboratory. S&T identified several planned research efforts that will involve the collection of PII and is preparing privacy compliance documentation for those projects.
- Established an internal Privacy Working Group to identify privacy-sensitive systems and research efforts, encourage coordination of privacy compliance efforts across S&T components, and collect S&T privacy questions and concerns to convey to the DHS Privacy Office.

Additionally, the S&T PPOC completed training and earned the Certified Information Privacy Professional /Government (CIPP/G) certification awarded by the International Association of Privacy Professionals.

3.4.3. S&T Privacy Policy

S&T drafted and implemented an S&T Privacy Policy on protecting PII. The policy provides guidance on the proper handling of PII, the use of a Privacy Act Statement when requesting PII, and requirements for information technology systems that handle PII. The policy also outlines the responsibilities of S&T employees and contractors with respect to protecting PII and describes the penalties associated with failing to properly protect PII.

In addition to its overall privacy policy, S&T completed the following specific policy activities:

- S&T General Counsel conducted a thorough legal analysis of the use of PII in social science research and provided the analysis to the DHS Privacy Office and DHS General Counsel.
- S&T established processes to coordinate privacy reviews for compliance with the Paperwork Reduction Act (PRA), C&A requirements, and records retention requirements.
- S&T also contributed subject-matter experts to DHS Privacy Office workshops on Closed Circuit Television (CCTV) and data mining.

3.5. Transportation Security Administration

The TSA Privacy Officer is responsible for developing privacy policies affecting a broad spectrum of the traveling public, transportation industry workers, and TSA employees, and ensuring TSA compliance with applicable privacy laws and regulations in coordination with TSA offices and the DHS 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 Office regularly meets with program leadership to ensure that privacy considerations are carefully considered prior to implementing or changing TSA programs. In addition, the TSA Privacy Office conducted outreach with biometric industry representatives and Federal, state and local law enforcement and security agencies. The TSA Privacy Office also attended the Computers, Freedom, and Privacy Conference on May 22, 2008, one of the most influential and widely attended annual privacy advocacy events.

During the past year, TSA augmented its professional privacy staff and continued to serve as the driving force behind a variety of data protection initiatives. Below are highlights of the TSA Privacy Officer's regulatory and policy activities during this reporting period.

3.5.1. Secure Flight

TSA's Secure Flight initiative implements the requirement in Section 4012 of the *Intelligence Reform and Terrorism Prevention Act* (IRTPA)[21] of 2004 to move responsibility for air passenger watch list matching from aircraft operators to the Federal government. TSA published its NPRM for the Secure Flight program in August 2007 and received comments from industry stakeholders, privacy advocacy groups, and the public regarding the proposed rule. In addition to the standard channels for receiving comments, TSA also received comments during a public meeting held in September 2007, attended by the TSA Privacy Officer, the Assistant Secretary for TSA, and several agency representatives. The comment period for the NPRM closed in November 2007, and TSA is in the last stages of finalizing the regulation.

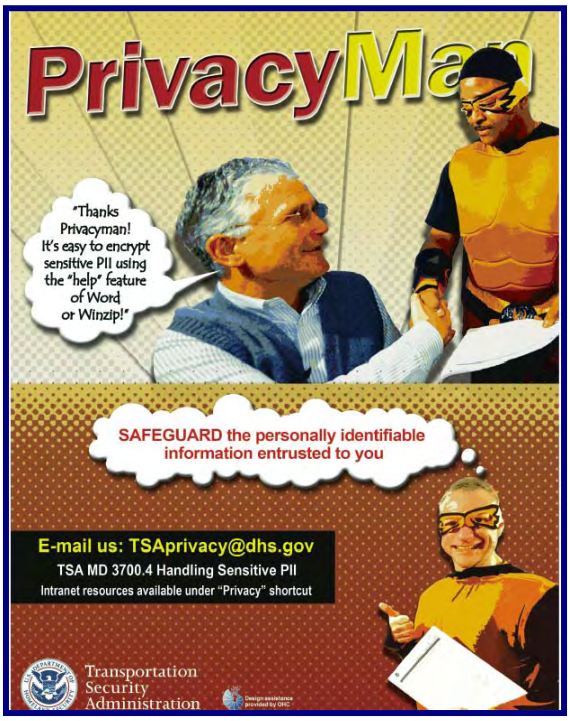
Secure Flight has made significant progress towards maturing its understanding and implementation of a robust privacy program that supports the program mission while mitigating risks to individual privacy. To this end, Secure Flight hired a privacy officer for the program and contracted for an integrated team of privacy professionals consisting of policy, operations, and technical experts deployed throughout the program. Working in concert with the new privacy officer for Secure Flight, the TSA Privacy Officer, and officials from the DHS Privacy Office, the Secure Flight privacy team identified risks and appropriate mitigation strategies. The team also published privacy notices including a PIA, SORN, Privacy Act Exemption NPRM, and PRA notice, which were released in conjunction with the Secure Flight NPRM. Since the NPRM publication, the privacy team has published the Privacy Act Exemption Final Rule and submitted the NARA Notice, which outlines the data retention schedule, for approval. These documents will also be updated and re-published with the Secure Flight Final Rule as appropriate. The team also works to ensure that the program continues to operate within the structure of currently published notices during its on-going development.

3.5.2. Handling Sensitive Personally Identifiable Information

TSA promulgated a Management Directive (3700.4) that established TSA policy and procedures for handling sensitive PII. This directive received praise throughout DHS and external agencies for the succinct, understandable guidance it provides employees on this critical area. This directive applies to all TSA employees and contractors, and applies only to PII that is considered sensitive because of the combination of PII elements that expose individuals to the risk of identity theft or other harms in the event of loss. It addresses multiple issues consisting of, but not limited to, physical security, electronic transmission, mobile device protection, safeguarding PII outside of DHS facilities, and the destruction of sensitive PII.

[21] Public Law 108-458.

To further promote procedures for handling sensitive PII, TSA launched the *Privacy Man* awareness campaign. The campaign consists of a series of posters depicting the *Privacy Man* characters in discussions with personnel regarding important issues, such as determining whether data is Privacy Act protected, reminding users of important practices, and providing information on where to find relevant policies. An example of one of the *Privacy Man* poster appears at right.



3.5.3. TSA IT Security Supporting Privacy

TSA scored the first-ever A+ rating on the DHS FISMA Scorecard – the Department's tool named for the FISMA requirements used to measure information system security of every Federal agency. The award follows in TSA's tradition of high standards – last year TSA was the only DHS component to receive an "A" score for its FISMA report. In addition to its system security requirements, FISMA directs Federal departments to identify IT and privacy risks intrinsic to each of its systems, develop ways to mitigate those risks, and report results of ongoing system assessments to OMB. TSA has led DHS components in adherence to these compliance requirements despite having one of the largest inventories of systems in DHS. The working partnership developed between the TSA Privacy and IT Security offices reinforces the agency's adherence to privacy principles throughout the life-cycle of its information systems. The IT Security Office plays a vital role in educating program managers about security measures, Federal mandates, and government-wide best practices to secure agency data.

3.6. United States Coast Guard

To promote awareness, the USCG conducted its first *Privacy Awareness Week*, April 28 through May 2, 2008. The PPOC hosted a Privacy Booth in the cafeteria at USCG Headquarters, which provided educational materials focusing on the need to safeguard PII and posters to place near copiers. USCG Privacy staff was available at the booth to answer questions. In addition, selected commands conducted an *All Hands Training*, in which Commanding Officers gathered their unit personnel and disseminated information on topics such as the need to safeguard PII within workstations.

The PPOC regularly advises USCG personnel or units affected by a privacy incident to review instructions and directives relating to statutory requirements, PIAs, SORNs, safeguarding PII, and incident reporting procedures.

The PPOC further implemented privacy compliance practices by reviewing all new and existing USCG directives, manuals, and policy documents prescribing compliance, safeguarding measures, and incident handling directions for all documents relating to PII.

The Coast Guard conducts its mandatory *Privacy Awareness Training* through the Coast Guard's online Learning Portal. The portal is accessible to active-duty, Reserve, Auxiliary, civilian employees (including Non-Appropriated Funds employees), and contractors who hold an active user account for a USCG Standard Work Station (SWS). The Coast Guard's 40,000 personnel are also provided a quick reference of *Dos and Don'ts* for protecting and handling personal data via the USCG's interactive intranet website. In an effort to extend privacy efforts even further, the Privacy Staff published an article in the *Reserve Magazine* entitled, *Privacy: A Look at Why It's Everyone's Responsibility.*[22]

Additionally, the DHS Privacy Office worked closely with the USCG on a PIA, SORN, NPRM, and Final Rule for the Law Enforcement Intelligence Database (LEIDB). LEIDB archives text messages prepared by individuals engaged in USCG law enforcement, counter terrorism, maritime security, maritime safety, and other Coast Guard missions enabling intelligence analysis of field reporting.

3.7. NPPD US-VISIT

The NPPD's US-VISIT Privacy Office stated mission is to uphold the privacy of individuals while protecting the nation's borders by adhering to the letter and spirit of U.S. privacy laws. US-VISIT adopted and complies with the fair information practice principles by treating individuals and their personal information with respect, and by ensuring a high standard of privacy protection. Since its inception, the US-VISIT Program has been a strong and dedicated proponent of privacy protection. This is clearly evident as US-VISIT identifies safeguarding privacy as one of its four program-level goals. US-VISIT's Increment 1 deployment PIA was the first PIA conducted by DHS, and the US-VISIT Program continued to demonstrate its dedication to privacy during this report period by publishing five PIAs and two SORNs.

US-VISIT has a dedicated Privacy Officer and a team of privacy analysts. The US-VISIT Privacy Officer is responsible for compliance with all applicable privacy laws, regulations, and US-VISIT privacy requirements. The US-VISIT Privacy Officer builds and supports a culture that values privacy within the US-VISIT Program. One of the ways this is implemented is by training new employees in privacy protection and conducting annual refresher privacy training. Moreover, the US-VISIT Privacy Officer and the privacy team are involved in all new projects within the US-VISIT Program, from the early stages through the execution stage, and continuing for the duration of the project's operations and maintenance. The US-

[22] *The Reservist*, May 2008: 26+; Vol 55/Issue 4-08.

VISIT Privacy Officer was instrumental this year in introducing a privacy awareness campaign to increase Federal employees' and contractors' awareness of the importance of privacy protection of the data entrusted to them.

The US-VISIT Program website includes specific web pages dedicated to privacy. The US-VISIT Privacy Protections and Protocols website is available at www.dhs.gov/xtrvlsec/programs/gc_1180020923182.shtm.

3.7.1. Protection of Traveler Privacy through Privacy Compliance

Safeguarding the privacy of visitors to the United States is a primary goal of US-VISIT. As part of meeting this goal, US-VISIT handles all PII of non-U.S. citizens held in mixed systems in accordance with the FIPPs. Developments in the US-VISIT Program are evaluated and reflected in PIAs, SORNs, and updates to other relevant program privacy documentation as new US-VISIT projects are implemented. Examples of privacy compliance documents issued this year include:

- *Technical Reconciliation Analysis Classification* (TRACS). TRACS serves as a new information management tool used for case management and analysis of US-VISIT records for detecting, deterring, and pursuing immigration fraud, and identifying persons who pose a threat to national security and/or public safety. DHS published a PIA, SORN, and NPRM to support this program.

- *Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure* (Exit Program). The Exit Program is implementing the first phase of the Exit component of its integrated, automated biometric entry-exit system that records the arrival and departure of covered aliens; conducts certain terrorist, criminal, and immigration violation checks of covered aliens; and compares biometric identifiers to those collected on previous encounters to verify identity. US-VISIT published the Exit PIA to support this program.

- *Arrival and Departure Information System* (ADIS). US-VISIT republished a SORN for ADIS. This SORN was updated primarily to add a routine use to cover sharing of ADIS data with intelligence agencies in support of the DHS mission to identify and prevent acts of terrorism against the United States. Revisions also included revising the category and sources of records sections to clearly indicate that some data may come from foreign governments and a proposal to reduce the retention period from 100 to 75 years. US-VISIT published a PIA update for ADIS, which described changes to ADIS corresponding to the publication of the new ADIS SORN. US-VISIT also published a NPRM for ADIS in the Federal Register, proposing to exempt this system of records from certain provisions of the Privacy Act due to criminal, civil, and administrative enforcement.

As the program expands and provides its identity management services to additional entities, US-VISIT will continue to publish PIAs, PIA updates, and SORNs in order to maintain program transparency and give the public advance notice and continued insight into the workings of the program.

3.7.2. Responding to Requests for Redress

US-VISIT was a pioneer in providing foreign travelers an opportunity to seek redress. US-VISIT developed and implemented a well-publicized redress process to provide individuals with a straightforward mechanism for review of the personal information collected about them, to have information corrected as appropriate and, if desired, appeal redress decisions to the DHS Chief Privacy Officer.

The US-VISIT Privacy Office replies to redress requests it receives directly and also supports the DHS Traveler Redress Inquiry Program (TRIP) system for receipt and processing of redress inquiries. Most US-VISIT redress inquiries are (1) requests for access to or correction of personal records maintained by US-VISIT, or (2) requests for access to or correction of records outside the purview of US-VISIT.

During the report period, US-VISIT received and handled 157 US-VISIT specific redress requests and issued responses to the requestors. The US-VISIT specific redress requests processed this year significantly increased, representing almost half of the total US-VISIT specific redress requests (345) received since its inception in January 2004.

4. Implementing Recommendations of the 9/11 Commission Act

On August 3, 2007, President Bush signed the *Implementing Recommendations of the 9/11 Commission Act of 2007*[23] (the "9/11 Commission Act"). This law significantly added to the authority and responsibilities of the DHS Chief Privacy Officer. The sections that follow discuss the significant impacts of the 9/11 Commission Act.

4.1. Section 802: Authority of DHS Chief Privacy Officer

Section 802 of the 9/11 Commission Act amended Section 222 of the Homeland Security Act, which statutorily created and defined the role of the DHS Chief Privacy Officer. Most significantly, Section 802:

- Codifies the authority of the Chief Privacy Officer to investigate and or report on DHS programs and operations with respect to privacy. The section contains authorities consistent with the powers granted by the Secretary to the Chief Privacy

[23] Public Law 110-53.

Officer under DHS Management Directive 0470.2, *Privacy Act Compliance*, including granting the authority to:

  - Exercise his or her own discretion in deciding which programs to investigate or report on, and to facilitate these investigations
  - Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to privacy within the programs and operations
- Grants the Chief Privacy Officer two new investigative authorities, including the power to:
  - Issue subpoenas to any person other than a Federal agency, with the approval of the Secretary; and
  - Administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to his or her responsibilities under Section 222 of the Homeland Security Act.
- Establishes formal requirements for coordinating investigations of violations or abuse related to privacy within the Department with the DHS Office of Inspector General (OIG). See Section 9.3 of this report for additional information regarding the interactions between the DHS Privacy Office and the OIG.

The text of the amended Section 222 of the Homeland Security Act is available on the DHS Privacy Office website.[24]

4.2. Section 803: Authority of Federal Privacy Officers/Privacy Officers to Report

Section 803 of the 9/11 Commission Act creates a new reporting requirement for select privacy offices within the Federal Government, including the DHS Privacy Office.[25] Each quarterly report submitted under this section contains information on: (1) the number and types of reviews undertaken by the Chief Privacy Officer; (2) the type of advice provided and the response given to such advice; (3) the number and nature of the complaints received by the Department for alleged violations; and, (4) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

The Chief Privacy Officer submitted the first two quarterly reports required under Section 803 of the 9/11 Commission Act during this reporting period. Copies of these reports are

[24] See www.dhs.gov/privacy, then follow the links to "About the Privacy Office."

[25] See 42 U.S.C. 2000ee-1.

available on the DHS Privacy Office website, and they are discussed in Sections 9 and 17.1 of this report.[26]

4.3. Section 804: Data Mining

This section of the 9/11 Commission Act, entitled *Federal Agency Data Mining Reporting Act of 2007*, requires all Federal agencies engaging in data mining to report their activities annually to Congress. The Act provides a new definition of "data mining" and specifies content areas that must be addressed for each data mining activity included in the report. DHS's data mining activities and reports are discussed in more detail in Sections 12.3.3 and 17.2 of this report.

4.4. DHS Privacy Office support for other initiatives

In addition to Sections 802 and 803, which dealt explicitly with the authority of the Chief Privacy Officer, a number of other sections of the 9/11 Commission Act call on the DHS Privacy Office to conduct PIAs of various programs and provide privacy training to program participants. These requirements are described in the following sections.

4.4.1. DHS State, Local, and Regional Fusion Center Initiative

Section 511 of the 9/11 Commission Act establishes the fusion center initiative, codifying the efforts of the State and Local Program Management's Office (SLPMO) within DHS's I&A Directorate. This section amended the Homeland Security Act by adding a new section 210A [6 U.S.C. 124h]. Section 511 contained a number of provisions specifically related to privacy, including:

- *PIA requirement*. Section 511(d)(1) called for a Concept of Operations, to include a PIA. Although this took longer than the 90 days articulated in the Act, the SLPMO and DHS Privacy Office staff made substantial progress on this report, including the PIA, during the reporting period. The draft PIA along with the Concept of Operations will be issued shortly.

- *Subsequent Privacy Report*. Section 511(d)(2) requires the DHS Privacy Office to submit a report on the privacy impact of the program one year after the enactment of the Act. This requirement will be addressed during the next annual reporting period.

- *Privacy training for I&A intelligence analysts assigned to a fusion center*. Section 511(c)(4)(A)(ii) requires I&A analysts assigned to a fusion center to receive "appropriate" privacy training "in coordination with the Chief Privacy Officer" for all State, local, tribal, and private sector representatives at the fusion center. The DHS

[26] Section 803 reports are found on the Privacy Office website, www.dhs.gov/privacy, then follow links to "Reports and Statements."

Privacy Office teamed with the DHS CRCL, which has a similar training mandate, to provide targeted privacy and civil liberties training to these I&A analysts. During the reporting period, the DHS Privacy Office distributed its *Introduction to the Culture of Privacy* CD-ROM to all analysts currently assigned to a fusion center. Following this, the DHS Privacy Office conducted the first of two two-hour privacy and civil liberties training sessions, narrowly tailored to the issues analysts could face during their fusion center assignments. On the privacy side, this first session focused on an introduction to Federal privacy law, including the Privacy Act, the E-Government Act, and a discussion of the FIPPs. The instruction then examined the particular systems the analysts would access and the published SORNs which govern the use of the information in those systems. The DHS Privacy Office also developed content for a second two-hour class, which provides instruction regarding rules for handling PII and data breach protocols. This material will be presented to the analysts during the next reporting period. Moreover, this entire four-hour curriculum is available for each candidate I&A plans to assign to a fusion center in the future.

- *Privacy training for State and local fusion center representatives*. Section 511(i)(6) requires the Department to ensure fusion centers provide "appropriate" privacy training "in coordination with the Chief Privacy Officer." Once again, the DHS Privacy Office teamed with CRCL to fulfill this responsibility. In addition, these two offices joined forces with the Bureau of Justice Assistance (BJA) within DOJ and the Program Manager of the Information Sharing Environment (PM-ISE) to develop content in order to train the trainers. The parties anticipate delivering this content during the next reporting period.

- *Information Sharing Environment*. Section 511(i)(3) places fusion centers sharing terrorism information within the scope of the Information Sharing Environment (ISE). The PM-ISE requires that fusion centers adopt privacy protections that are "at least as comprehensive" as Federal agency participants. The ISE is discussed in more detail in Section 13.1 of this Annual Report.

4.4.2. Information Sharing Fellows Program

Section 512 of the 9/11 Commission Act establishes the Information Sharing Fellows (ISF) Program.[27] Under the ISF, State, local and tribal Law Enforcement Officers (LEOs) and intelligence analysts will be detailed to the Department to participate in the work of I&A in order to become familiar with (1) the relevant missions and capabilities of the Department and other Federal agencies, and (2) the role, programs, products, and personnel of I&A. In addition, the program is designed to promote information sharing between the Department and State, local, and tribal LEOs and intelligence analysts by assigning such officers and analysts to:

[27] New section 210B of the Homeland Security Act [6 U.S.C. 124i].

- Serve as a point of contact in the Department to assist in the representation of State, local, and tribal information requirements;
- Identify information within the scope of the ISE that is of interest to State, local, and tribal LEOs, intelligence analysts, and other emergency response providers;
- Assist Department analysts in preparing and disseminating products derived from information within the scope of the ISE that are tailored to State, local, and tribal LEOs and intelligence analysts, and designed to prepare for and thwart acts of terrorism; and
- Assist Department analysts in preparing products derived from information within the scope of the ISE that are tailored to State, local, and tribal emergency response providers, and assist in the dissemination of such products through appropriate Department channels.

This program also contains a number of provisions specifically addressing privacy, including:

- *PIA requirement*. Section 512(c)(1) calls for a Concept of Operations which includes a PIA. On April 14, 2008, the Chief Privacy Officer signed a PIA for the Information Sharing Fellows program. This PIA examined the program's implementation of the FIPPs. This PIA, like all PIAs of the Department, will be updated as necessary in the future.
- *Subsequent Privacy Report*. Section 512(c)(2) requires the DHS Privacy Office to submit a report on the privacy impact of the program one year after the enactment of the Act. This requirement will be addressed during the next annual reporting period.
- *Privacy training for Information Sharing Fellows*. Section 512(b)(1)(E) states that in order to be eligible for the program, candidates need to undergo privacy training developed, supported, or sponsored by the DHS Chief Privacy Officer. As with the fusion center program, the DHS Privacy Office and CRCL teamed up during the reporting period to develop training targeted to these individuals and the particular privacy issues they will face. Training will begin in the next reporting period as candidates are identified.

4.4.3. Interagency Threat Assessment and Coordination Group

Section 521 of the 9/11 Commission Act creates the Interagency Threat Assessment Coordination Group (ITACG).[28] The ITACG is comprised of State, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed and assigned to work at

[28] New section 210D of the Homeland Security Act [6 U.S.C. 124k].

the National Counterterrorism Center (NCTC) with Federal intelligence analysts for the purpose of integrating, analyzing, and assisting in the dissemination of Federally-coordinated information within the scope of the ISE. This section of the 9/11 Commission Act discusses:

- *PIA requirement*. Section 521(c) requires a PIA. Because the ITACG is a multi-agency effort, the PIA is a joint product of the DHS Chief Privacy Officer, the Chief Privacy and Civil Liberties Officer of the Department of Justice, in consultation with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI). This PIA examines the program's implementation of the FIPPs.
- *Privacy training for members of the ITACG*. Section 521(g)(2)(E) requires all members of the ITACG detailed to NCTC to receive appropriate privacy training developed, supported, or sponsored by the DHS Chief Privacy Officer. As with the fusion center program, the DHS Privacy Office and CRCL teamed up during the reporting period to develop training targeted to these individuals and the particular privacy issues they will face. Training will begin in the coming reporting period for assigned officers and identified candidates.

4.5. DHS Privacy Office Support for Other Programs

In addition to the support described in the previous sections, the 9/11 Commission Act also requires the DHS Privacy Office to support the following programs:

- *Rural Policing Institute*. Section 513 establishes the Rural Policing Institute within the Federal Law Enforcement Training Center (FLETC). The section further provides that the institute shall include classes about the protection of privacy.
- *R&D Program to improve Public Transportation Security*. Section 1409 instructs the Department, through S&T, to carry out a research and development (R&D) program to improve public transportation security in consultation with TSA and the Department of Transportation (DOT). Under subsection (d)(1) and (2), the Secretary of Homeland Security shall consult with the Chief Privacy Officer, who shall conduct a PIA if appropriate.
- *R&D Program to improve Railroad Security*. Section 1518 establishes the Railroad Security R&D program within S&T, in consultation with TSA. Under subsections (d)(1) and (2), the Secretary of Homeland Security shall consult with the Chief Privacy Officer, who shall conduct a PIA if the Secretary determines the program will have an impact on privacy.
- *Northern Border Railroad Passenger Report*. Section 1523(b)(2) requires the Department to publish a report on a number of particulars relating to the prescreening of passengers and freight on railroads (and airlines) on both sides of the U.S. border with Canada. Under Subsections (b)(1) and (2), the Secretary of Homeland Security shall consult with the Chief Privacy Officer on the preparation of the report, which

shall include a PIA. During the reporting year, the DHS Privacy Office and CBP made substantial progress on the PIA, which is scheduled for publication in the next reporting year.

- *R&D Program to improve security of Over-the-Road Bus Transportation.* Section 1535 establishes the R&D program to improve over-the-road bus security. S&T shall manage the program in consultation with TSA. Under subsections (d)(1) and (2), the Secretary of Homeland Security shall consult with the Chief Privacy Officer, who shall conduct a PIA if the Secretary determines the program will have an impact on privacy.

Soon after the 9/11 Commission Act was signed by the President, Secretary Chertoff established the DHS 9/11 Act Working Group. Co-chaired by the Office of Policy and Office of the General Counsel, the group assembles nearly 30 component and office representatives in order to facilitate coordination of responsibilities and consolidate reporting. The DHS Privacy Office sits on this working group, provides regular status updates of the tasks assigned it, and attends monthly meetings to ensure the Departments' new statutory obligations are implemented thoroughly, and in a timely manner.

5. Fusion Centers

As discussed in Section 4.4.1, significant portions of the 9/11 Commission Act focused on the Department's fusion center program and, in particular, steps participants must take to ensure their activities promote the privacy interests of individuals in the communities they serve. The fusion center program, however, predates the 9/11 Commission Act, and the DHS Privacy Office was already closely engaged with the SLPMO to build privacy protections into the program at all levels. The DHS Privacy Office's continued support for the program goes beyond the minimum requirements laid out in the 9/11 Commission Act.

In 2006, Secretary Chertoff signed the *DHS State and Local Fusion Center Support Implementation Plan* and designated the Chief Intelligence Officer as the executive agent for the Department's interactions with and support to fusion centers. Under this authority, I&A began assigning senior intelligence analysts to State and local fusion centers around the country. At the same time, the program engaged the DHS Privacy Office to help determine how to share information in two directions with the fusion centers while complying with the Privacy Act, and in a manner consistent with the FIPPs.

The Chief Privacy Officer addressed a plenary session of the National Fusion Center Conference in San Francisco, California. Nearly 800 attendees—representing fusion centers across the Nation, Federal fusion center partners, Congressional staff, and others—heard the Chief Privacy Officer stress the importance of establishing a robust privacy program in each fusion center by employing the resources developed by the PM-ISE. He cautioned the audience about the negative consequences of ignoring privacy issues, illustrating his point with examples

where programs lost the support of the public and were cancelled because they neglected to establish adequate privacy protections or failed to follow their own policies. Finally, the Chief Privacy Officer reviewed the responsibilities of the DHS Privacy Office within the 9/11 Commission Act and praised the partnership between I&A, CRCL, and the DHS Privacy Office, and between DHS, DOJ, and PM-ISE to create and deliver privacy training for fusion centers.

A DHS Privacy Office representative attended the Southern Shield fusion center conference in Nashville, Tennessee. He delivered an introduction to Federal privacy law, the FIPPs, the ISE, and urged the fusion centers to appoint an in-house privacy official, educate themselves on their own jurisdiction's privacy framework, and provide privacy training for all fusion center employees. Finally, he recommended that each fusion center utilize the Global Justice Fusion Center Guidelines, a powerful resource issued jointly by DHS and DOJ's Bureau of Justice Assistance. Senior Office staff also toured and discussed privacy protections at fusion centers in Jacksonville and Tallahassee, Florida; Atlanta, Georgia; Baltimore, Maryland; Las Vegas, Nevada; and Centennial, Colorado.

The Office participated in introducing to the fusion centers the Global Justice Fusion Center Guidelines,[29] a powerful resource issued jointly by DHS and the DOJ's Bureau of Justice Assistance. The Global Guidelines provide methods to address privacy concerns throughout the document. Global Guideline 3, for instance, urges the inclusion of a privacy committee in the fusion center governance structure. Global Guideline 5 recommends the use of Memorandum of Understanding (MOUs) between information sharing partners that address privacy and security principles. Global Guideline 8 is dedicated to promoting meaningful and lawful privacy policies at the fusion centers, and to providing mechanisms ensuring that the centers adhere to these policies. This begins with consideration of the FIPPs, which are the worldwide baseline for privacy protection.

The Fusion Center Guidelines provide a useful list of complementary elements for the privacy policy drafters and include the following:

- Add introductory language that clearly states the privacy practices of the center;
- Describe the information collected and how the information is stored;
- Establish a common lexicon of terms for dealing with role-based access;
- Define and publish how the information will be used;
- Draft a clear, prominent, and understandable policy;
- Display the privacy policy for both center personnel and customers;

[29] These guidelines are available in the Fusion Center Guidelines posted on the Institute for Intergovernmental Research: http://www.iir.com/global/products/fusion_center_guidelines_law_enforcement.pdf.

- Ensure that all other policies and internal controls are consistent with the privacy policy;
- Establish a business practice of notifying government agencies of suspected inaccurate data;
- Adhere to applicable State and Federal constitutional and statutory civil rights provisions;
- Partner with training centers on privacy protection requirements and conduct periodic privacy security audits;
- Consult with the privacy committee (established pursuant to Guideline 3) to ensure that citizens' privacy and civil rights are protected;
- When utilizing commercially available databases, ensure that usage is for official business and the information is not commingled with private sector data. To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data; and
- Determine if there are security breach notification laws within the jurisdiction and follow those laws, if applicable.

The remainder of Guideline 8 focuses on the measures that leaders of each fusion center should take to ensure the policy is followed. These steps include such prudent steps as ensuring adequate training, conducting information privacy awareness activities, and establishing a policy for tracking and reviewing privacy complaints and concerns.

Global Guideline 9 provides a framework for ensuring adequate security measures are in place. This includes security for facilities, data, and personnel. Following these security recommendations will ultimately serve privacy by protecting data from unauthorized access.

The DHS Privacy Office continues to support both the use of the Global Guidelines by the fusion centers as well as the evolution of the Guidelines as the PM-ISE generates its requirements for sharing homeland security related information with fusion centers.

The DHS Privacy Office is committed to enhancing transparency in the fusion center program. As discussed in Section 14, the DHS Privacy Office held a public meeting of its Data Privacy Integrity and Advisory Committee (DPIAC) during the reporting year dedicated almost entirely to the subject of fusion centers and privacy. A member of the DHS Privacy Office also attended the Southwest Regional Fusion Center Conference, on November 6, 2007. Following the presentation on the ISE, the DHS Privacy Office representative helped introduce a tool designed to assist fusion centers in drafting their Privacy and Civil Rights Policies.

The DHS Privacy Office will continue its substantial involvement with the fusion center program during the next reporting year.

6. Credentialing and Verification Programs

The DHS Privacy Office continued to work on privacy issues related to a number of credentialing and verification programs, including REAL ID, the Western Hemisphere Travel Initiative (WHTI), TRIP, Homeland Security Presidential Directive 12 (HSPD-12), and E-Verify. The following sections discuss the DHS Privacy Office's activities regarding each of these programs.

6.1. REAL ID

As reported in last year's Annual Report, Congress passed the *REAL ID Act of 2005*[30] to set minimum requirements for state issuance of drivers' licenses and identification cards required for "official purposes." The REAL ID rulemaking and implementation continued to be an important policy area for the DHS Privacy Office this year. The REAL ID rule seeks to combat false forms of identification by implementing uniform standards that enhance the integrity and reliability of drivers' licenses and identification (ID) cards, strengthen identity verification capabilities, and increase security at drivers' license and ID card production facilities.

The DHS Privacy Office participated in the review of more than 20,000 public comments filed in response to the Department's NPRM and initial PIA issued in March of 2007. DHS issued the final rule on January 11, 2008. The REAL ID final rule sought to lower the cost of REAL ID and set a phased implementation schedule for the states. States were required to apply for an extension by March 31, 2008, and full compliance was extended to December 1, 2017. The final rule also addressed a number of the concerns that were raised in the NPRM PIA. First, it assured the public that the rule would not lead to a national ID as the states would continue to issue the drivers' licenses and each state could set its own numbering system. Second, in response to concerns about the security of the state databases, DHS assured the public that it will monitor state compliance with Federal information security standards. Third, the final rule also required states to create and implement security plans for protecting PII.

In conjunction with the final rule, the DHS Privacy Office issued a PIA, which outlined the changes made to the proposed rule and discussed the remaining privacy issues. The PIA identified continuing concern regarding the states' implementation of the data verification processes resulting from the new rule. Specifically, the PIA inquired how the states' Departments of Motor Vehicles (DMVs) will conduct and govern the data verification of Federal databases and how they will conduct and govern the state-to-state check to determine whether an applicant for a REAL ID card holds a driver's license in another state. Additionally, the PIA expressed concerns about third parties' access and use of PII stored on a REAL ID credential, since no encryption is required, and whether third parties will use REAL ID for purposes other than those expressly outlined in the act.

[30] Public Law 109-13.

In tandem with the PIA, the DHS Privacy Office also issued a set of *Best Practices for the Protection of PII* to provide guidance to the states' DMVs on privacy and security protections consistent with the Privacy Act, FISMA, and the information security standards developed by the National Institute of Science and Technology (NIST). Both the final rule and the PIA, which includes the Best Practices guide, can be found on the DHS Privacy Office website.[31] The DHS Privacy Office will continue to work with the REAL ID Program Office to ensure the implementation of the final rule is consistent with the FIPPs.

6.2. Western Hemisphere Travel Initiative

One of the goals of the DHS WHTI program is to reduce the potential for an individual to gain access into the United States by falsely claiming to be a U.S. or Canadian citizen. WHTI designates a limited set of secure documents acceptable for entry into the United States and incorporates the latest security technology at land ports of entry to expedite the CBP inspection process. The initiative, which is scheduled to go into effect on June 1, 2009, at land and sea ports of entry, will require individuals previously exempt from presenting documents (U.S., Canadian, and Bermudan citizens) to present a valid passport or other accepted document that establishes the bearer's identity and citizenship when entering or departing the United States from within the Western Hemisphere. WHTI closes regulatory exceptions to the passport requirements that were previously contained in the Immigration Nationality Act (INA). CBP will maintain all border crossing information in the Border Crossing Information System, which resides on the Treasury Enforcement Communication System (TECS) platform. The SORN for TECS is published at 66 Fed. Reg. 53029, and the Border Crossing Information System SORN was published as a separate system on July 25, 2008, at 73 Fed. Reg. 43457, to provide additional transparency as well as access and amendment rights.

The DHS Privacy Office issued a PIA on the WHTI notice of proposed rule making on August 10, 2007, and issued a PIA on the final rule on March 24, 2008, noting that WHTI did not create a new collection of data elements, but rather permitted the same information from additional categories of individuals to be collected. U.S. citizens can present a Department of State-issued passport or "passport card." The passport card uses a vicinity-read radio frequency identification (RFID) chip. With this technology, CBP officers will be able to access photographs and other biographical information stored in secure government databases before the traveler reaches the inspection booth to facilitate border inspection. For privacy protection, no personal information is stored on the electronic chip itself. The chip only has a unique number pointing to a stored record contained in secure government databases. The passport card is less expensive and more portable than a passport.

Several states are either issuing or planning to issue Enhanced Drivers Licenses (EDLs) as an alternative to passports and the passport card for land and sea travel. The EDL, along with

[31] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realidfr.pdf

the passport and trusted traveler cards,[32] uses RFID chip technology, which poses a number of privacy concerns. The DHS Privacy Office issued a PIA on RFID on January 22, 2008, which discusses the privacy concerns posed by RFID and how the Department is addressing them. Privacy advocates, however, continue to object to the use of RFID in the passport card and EDLs. On July 2, 2008, the DHS Privacy Office issued a PIA that explains the information technology and the information flow between the Border Crossing Information System, TECS, and other Privacy Act systems of records, including the Non-Federal Entity Data System (NEDS), which addresses EDLs. This PIA sheds important light on how the data collected from various sources at the border is handled. All PIAs are posted on the DHS Privacy Office website.[33] Section 8.1.1 discusses the RFID PIA in further detail.

6.3. Traveler Redress Inquiry Program

An important adjunct to the WHTI program is DHS TRIP. DHS TRIP serves 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 U.S. border crossings. It is a gateway, integrating individual DHS component redress programs, including TSA, CBP, USCIS, ICE, US-VISIT, CRCL, and the DHS Privacy Office. Travelers seeking redress are asked to provide information to assist DHS in resolving the underlying issue, which often involves misidentification of an individual. The online Traveler Inquiry Form allows individuals to detail their experiences. Significantly, TRIP is open to all individuals regardless of whether they are U.S. citizens, Lawful Permanent Residents, or simply visitors to the U.S. DHS TRIP's administrative process allows everyone, regardless of status, an avenue for redress they would not otherwise have under the Privacy Act. TRIP is one example of how DHS has implemented the Privacy Office's "mixed system" policy.[34] DHS TRIP received 31,206 redress requests for the period of July 31, 2007, through July 31, 2008.[35]

The DHS Privacy Office continues to provide guidance regarding DHS TRIP's handling of inquiries and is working with the other participating components to improve the program's operations. Most of the inquiries filed with the program that identify a privacy concern are complaints regarding the scope of border searches, the conduct of a border agent, or denied access to a flight. The DHS Privacy Office forwards these complaints to CBP to address.

[32] Trusted traveler cards include DHS-issued cards such as NEXUS, FAST, SENTRI.

[33] http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm

[34] DHS Privacy Policy Guidance Memorandum 2007-01 governs mixed use systems and provides for the extension of Privacy Act protections to PII of visitors and aliens.

[35] Of the requests received during the July 31, 2007, to July 31, 2008, timeframe, 2,100 were privacy related, meaning that the requester chose the "I feel my personal information has been misused," option.

6.4. Homeland Security Presidential Directive 12

On October 13, 2006, the DHS Privacy Office, in coordination with the Office of Security, published a PIA for the Personal Identity Verification (PIV) system. The DHS Privacy Office and Office of Security also published the Personal Identity Verification Management System (PIV MS) SORN supporting this effort.[36] The PIV system supports the Department's implementation of the Homeland Security Directive-12's (HSPD-12), which establishes a standard for identification of employees and contractors. HSPD-12 directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems. This initiative is intended to enhance security, increase efficiency, and reduce identity fraud. DHS is taking a phased approach to implementing HSPD-12, first bringing the Headquarters online, and then integrating the components.

Initially this effort and the privacy documentation will cover only Headquarters and any component using Headquarters credentialing processes. As part of the Department's ongoing HSPD-12 efforts, the DHS Privacy Office is working with the Office of Security to publish an update to the PIV PIA and the PIVMS SORN as components begin to use the Headquarters credentialing solution. The privacy documents for this expanded HSPD-12 implementation will be updated during the next reporting period to address integration with the components and to analyze any unique privacy issues presented as a result of the expansion.

6.5. E-Verify

In the fall of 2007, the Verification Division of USCIS established a new Privacy Branch to support the expansion of the E-Verify and Systematic Alien Verification for Entitlements (SAVE) programs. Because of the significant amount of personal information used by these programs, USCIS deemed it essential that the Verification Division have a dedicated staff of privacy professionals.

The E-Verify Privacy Branch provides policy analysis and development, staff training, and technical assistance to ensure privacy controls are built into system operations and procedures. The Privacy Branch also works to create a strong privacy outreach program, which includes working with the DHS DPIAC. The Privacy Branch is currently working with the DPIAC to improve various procedures for validating the identities of E-Verify users. Beyond establishing the Division's first Privacy Program, the staff completed several updates to the PIAs and SORNs to meet all Privacy Act requirements for new releases of the technology solutions supporting E-Verify and SAVE. These compliance activities allowed the Verification Division to maintain its aggressive schedule for program development, while continuing to ensure PII is protected and treated with the appropriate level of care.

[36] This SORN (DHS-OS-2006-047, September 12, 2006, 71 Fed. Reg. 53697) is available at: http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/E6-15044.htm.

7. Coordination with the Office of Civil Rights and Civil Liberties

Section 222(a)(5)(A) of the Homeland Security Act requires the Chief Privacy Officer to "coordinate[e] with the Officer for Civil Rights and Civil Liberties to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner." The Officer for Civil Rights and Civil Liberties has a matching obligation in Section 705 to coordinate efforts with the Chief Privacy Officer.

Both officers acknowledge the importance of maintaining a close working relationship due to the interrelatedness of their missions, and strive to give their authorities to cooperate maximum effect. To ensure free-flowing and regular exchange of information, staff members from the DHS Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL) began to hold regularly scheduled bi-weekly teleconference, giving the offices the opportunity to keep the other informed and seek advice and counsel where appropriate. In addition to this standing appointment, the offices have coordinated their efforts on a number of important tasks.

One key example of coordination between the DHS Privacy Office and CRCL during the report year is the State and local fusion center training required by the 9/11 Commission Act. In response to this requirement, the DHS Privacy Office and CRCL entered into a training MOU with I&A. In fulfilling its responsibilities to train DHS personnel assigned to State and local fusion centers, the two offices conducted their training sessions together, so that these intelligence professionals received a total of four hours of specialized training on civil rights, civil liberties, and privacy. The two offices continue to work together to create content for State and local fusion center representatives, joining forces with the DOJ Bureau of Justice Assistance and the PM-ISE. This training is described in further detail in Section 4.4.1 of this report.

When CRCL developed its Civil Liberties Impact Assessment (CLIA) during the reporting year in response to a Congressional mandate, the DHS Privacy Office shared its insights on its own PIA process. Following this, the Chief Privacy Officer invited the Officer for Civil Rights and Civil Liberties to address a public session of the DPIAC about the role of his office. This was followed by a panel to discuss the new CLIA tool.

The DHS Privacy Office worked closely with CRCL on the CCTV workshop and best practices initiative. See Section 12.3.2 for further information on this project.

In March, in a show of collaborative spirit, CRCL invited the Privacy Office to a joint reception marking the two offices' five year anniversary. The DHS Privacy Office and CRCL will continue to strengthen this relationship over the coming reporting year.

8. Technology

As DHS transitions from a need-to-know culture to a need-to-provide ISE, the DHS Privacy Office continues to evaluate the technologies that facilitate such enterprise sharing. Section 221 of the Homeland Security Act details the procedures that ensure the limitations, integrity, and security of the ISE. In addition, Section 222 positions the assessment of such technology and ensuring that technology does not erode privacy as a core responsibility of the DHS Chief Privacy Officer. While the DHS Privacy Office plays a pivotal role in vetting the technologies that contribute to information sharing, the Office also collaborates with S&T and numerous DHS components to determine suitable design considerations for integrating robust privacy protections into developing and operational technologies. With increasing demands in this area, the Office created a new position of Associate Director for Technology. The sections that follow discuss several of the major technology privacy initiatives during this reporting period.

8.1. Radio Frequency Identification

8.1.1. RFID PIA

DHS selected RFID technology[37] to support the daily operations of CBP Officers working at land ports of entry. In January 2008, the DHS Privacy Office released a PIA regarding the use of RFID technology in border-crossing travel documents, highlighting the privacy protections CBP employed in use of these technologies.

Each cross-border travel document contains an RFID chip that holds only a unique identifier number, which CBP officers can read wirelessly using RFID readers. The RFID cards use vicinity technology, which restricts the range at which the card can be read to approximately 15 feet, a distance that mitigates a potential privacy risk inside the physical perimeter of the secured border-crossing station. Also, the transmitted unique number is neither derived from PII nor appears on the card. The RFID readers send the unique number through a secured data circuit to back-end computer systems to pull relevant PII about the traveler linked with that particular card. This information is used to initiate the border-crossing screening process and create a new database record of the traveler's border crossing. By accessing the appropriate record(s) in advance, the CBP officer can prepare to process the border crossing more efficiently.

DHS uses RFID technology in Trusted Traveler Program (TTP) cards. Department of State issued Passport Cards, Border Crossing Cards, and state and provincial EDLs. DHS is in

[37] RFID refers to a method and type of technology used for identification. Generally, RFID systems operate using three components: the RFID tag, the reader, and the back-end system. The tag is attached to the object of interest. As the tag crosses a threshold, it wirelessly transmits information to a reader. The reader triggers the transfer of the unique information from the tag and, through the back-end system, associates that information with other information to create a meaningful response to the reader. Specific uses of RFID are further explained in the relevant PIAs on the DHS Privacy Office website.

discussion with various Native American Tribes interested in developing Enhanced Tribal Cards. When a traveler applies for a cross-border travel document, DHS collects PII during the enrollment process to determine eligibility for card usage, and key PII (i.e., a photo, full name, citizenship, date of birth, etc.) is printed on the face of the card. Should the RFID reader be inoperable for any reason, the printed information allows CBP officers to perform visual verification to check for accuracy. This consistent visual verification also mitigates the risk of a fraudulently duplicated RFID card being used successfully because the person using the duplicated information would not match the information stored in the back-end system. Furthermore, the RFID card design mitigates privacy risks through the transmission of limited information: the only information exchanged in the RFID portion of the border-crossing event is the unique number assigned to the RFID-enabled card.

In addition, CBP educates RFID card users about the permissible uses of the RFID card, and the users receive a protective sleeve that blocks the transmission of the RFID number, mitigating the likelihood of a traveler somehow being tracked or profiled if the RFID number were transmitted unbeknownst to the traveler. For legitimate information sharing within DHS, all DHS personnel must establish a need to know the information, and CBP controls the data through the use of strict access controls for the users, passwords, background checks, and auditing systems that track and report access to data.

8.1.2. OECD Draft Policy Principles on Radio Frequency Identification

The Organization for Economic Co-operation and Development (OECD) Working Party on the Information Economy (WPIE) and the Working Party on Information Security and Privacy (WPISP) produced a joint draft of policy principles on RFID in November 2007. The DHS Privacy Office Technology Group collaborated with the International Privacy Policy Group to review the draft, which became finalized for the OECD Ministerial meeting in June 2008.

The policy principles draft recognizes the various complexities that lead to RFID having such large economic potential. RFID technology, exemplified by RFID-enabled passport cards used at border crossing stations, can be instrumental in streamlining some DHS processes. The participation of the DHS Privacy Office in developing these OECD principles offers an opportunity for our office to educate our international peers about DHS policies and approaches to incorporating privacy protections within such technological development. In its comments to the WPIE and WPISP on the drafted international principles, the DHS Privacy Office emphasized that privacy should not be conditional; rather, it should be as ingrained as security when considering how to implement a privacy management strategy for RFID systems.

Participating in the development of such principles establishes a voice for the DHS Privacy Office regarding the international perspective of the privacy concerns attached to the ever-increasing use of RFID technology. Participating in the cross-borders dialogue about such technology principles is central to upholding the DHS mission while collaborating with our international counterparts.

8.2. Biometrics and Identity Management

The DHS Privacy Office actively participated in a number of DHS initiatives that generally fall under the rubric of identity management. In each of these initiatives, the DHS Privacy Office focused on integrating the FIPPs and specific privacy protections to support the delivery of privacy protective technology solutions.

8.2.1. Person-Centric View Initiative

The DHS OCIO and the DHS Office of Policy's Screening Coordination Office (SCO) have the lead role in developing a foundation that will support a "person-centric view" of information within the Department. This initiative would create the ability to associate information about a person across DHS Components and encounters; harmonize component investments and programs; and streamline privacy, regulatory, and paperwork reduction access processes.

From the individual's perspective, "person-centric view" means that all the relevant information about him or her would be made available to a DHS officer or decision-maker in a single, integrated view - regardless of where the data is physically stored. Physically, data would not be held in one database or a single system. The data would still be controlled by the DHS Component or Program responsible for the original collection and primary use of the information. The person-centric view would enable other DHS components or programs to view the same distributed data on a single screen, supported by appropriate levels of availability, access speed, quality, and security.

Today, relevant information about individuals exists in multiple systems, in which data may be redundant, conflicting, not current, incomplete, and difficult to access. Access requirements and available analytics capabilities may vary from system to system and coordinated data governance is limited.

From the DHS perspective, a person-centric view gives decision-makers access to data for specific individuals using common data elements with customized views that meet each decision-maker's specific needs, without having separate logins to each system where it is held. This new capability will help DHS facilitate transactions with legitimate individuals while making accurate assessments about those who are high risk or ineligible. This initiative will also create an easy way for an individual to tell DHS that DHS has encountered him or her previously. It will also create an easy way for DHS to verify that the person they are working with is the one DHS has encountered previously.

There are a number of efforts required in order to implement the person-centric view. Several of these are described below:

- *Uniform approach to privacy compliance*. Privacy compliance documentation is a key requirement for this initiative and will be integrated into the operational processes

of these new services. This includes PTAs, PIAs, and SORNs. The Privacy Office is already working with several components, including USCIS and CBP, on how to develop PIAs associated with elements of the intended enterprise-level services in DHS's Service Oriented Architecture.

- *Standardized data collection.* Standardized collection of core biographic information will allow DHS to improve its ability to screen individuals (e.g., conduct checks against derogatory data) and match encounters. The five core biographic data elements are: name (last name, first name, middle name, and full name); date of birth; country of birth; gender; and country of citizenship. Recently, components were directed to conduct an assessment of the impact of standardized data collection of these five core biographic data elements on credentialing, screening, and law enforcement programs' business processes, information systems, forms, or other related activities. Components can request exceptions to the policy if a system is scheduled for retirement within two years, statutory authority specifically prohibits collection of additional information, or it can demonstrate that changes to business processes and supporting IT systems would be unduly onerous compared to the benefit of capturing the five data elements. The Privacy Office is working closely with the OCIO and SCO to ensure that this effort complies with all privacy documentation requirements.

- *Use of IDENT.* Another key departmental identity management effort is to have all DHS programs that require the collection and use of fingerprints to use the Advanced Biometric Identification System (IDENT) for storage and matching. The DHS Privacy Office worked with US-VISIT, the steward of IDENT, to ensure that the system complies with all privacy documentation governing the system.

8.2.2. Federal Biometrics & Identity Management Task Force

The Privacy Office continued its work as co-chair of the privacy working group of the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management. This year's effort focused on the Privacy Office's lead role in the Subcommittee's Task Force on Identity Management (IdM). The Task Force membership spans over a dozen Federal departments and agencies, illustrating the far-reaching impact of IdM technology. The Task Force reviewed existing IdM activities and technologies in public and private sectors and sought to establish baseline standards for ongoing and emerging IdM programs as well as recommendations regarding critical IdM issues that require both immediate attention and long-term action. In addition, as the Task Force considered flexible architecture that could sustain individual agency requirements, it assessed development of a Federal, standardized IdM taxonomy. The Privacy Office played an instrumental supportive role in the Task Force, offering a privacy compliance model that would support integration of privacy compliance requirements into the technology architecture of IdM deployments.

8.2.3. Biometrics Consortium Conference

The DHS Privacy Office and S&T staff attended the 2007 Biometric Consortium Conference held in Baltimore, Maryland. The DHS Privacy Office staff also made a presentation regarding the privacy concerns related to the use of biometrics and how to resolve those concerns pragmatically by embedding privacy into the operations of biometric programs and identity management architecture.

Overall, the conference highlighted government progress in using biometrics and collaborative efforts between the public and private sectors. These efforts are critical to greater biometric advancement, and such growth demands privacy protections for managing and developing the technology..

8.3. Whole Body Imaging

The *Aviation and Transportation Security Act* (ATSA),[38] directs TSA to conduct "research, development, testing, and evaluation of threats carried on persons boarding aircraft or entering secure areas, including detection of weapons, explosives, and components of weapons of mass destruction." As part of such development, TSA submitted a PIA to the DHS Privacy Office describing TSA's pilot operations for Whole Body Imaging (WBI) technologies, which include backscatter x-ray and millimeter wave devices designed to identify prohibited weapons or other objects during the physical screening process. The PIA described how the new technologies could affect the privacy of individuals that choose to undergo the voluntary screening. After completing its review, the DHS Privacy Office published the PIA in January 2008.

Although this new-found technology could pose privacy concerns stemming from the passenger images they capture, the manufacturers took steps to modify the technologies to address those concerns. Both WBI technologies were modified to reduce the photographic detail, such that the Transportation Security Officer (TSO) viewing the image can identify prohibited objects but not identify the person being screened. In addition, the millimeter wave device blurs the facial image viewable to the monitoring TSO, who stays in a remote viewing room, away from the actual WBI screening area. No photographic devices, including cell phone cameras, are permitted in the viewing room. The manufacturers have disabled image-storage functions in the WBI equipment, meaning an individual's image only remains visible to the screening TSO until the TSO clears that individual, after which the image is deleted to allow the next screening.

TSA invited representatives from a variety of privacy and civil liberties advocacy groups to view and assess the agency's Millimeter Wave Whole Body Imaging device prior to initiating

[38] Public Law 107-71.

a pilot test of the technologies. The interaction affirmed TSA's planned efforts to implement the critical privacy protections described in the WBI PIA.

The privacy-protecting mechanisms inherent in the design and implementation of these WBI technologies illustrates the commitment of TSA and the DHS Privacy Office to meet the directives of the ATSA in a manner that minimizes privacy intrusions while helping keep prohibited items outside secured airport areas. The WBI PIA embodies all of the FIPPs, particularly the principle of transparency, which led to this PIA. TSA also published an online publication of WBI technology information and conducted outreach with national press and privacy advocacy groups during the pilot's development.

8.4. Service Oriented Architecture

The DHS Privacy Office has worked collaboratively with various components to standardize how the Department integrates privacy protections into their respective Service Oriented Architecture (SOA) deployments across the components. In particular, the DHS Privacy Office is developing a three-tiered approach, which divides SOA system privacy compliance documentation into Client, Service, and System roles. Components can conduct separate PIAs at each level and reuse base templates for new Client/System combinations.

Such standardization will become increasingly important as DHS pushes toward an Enterprise Architecture across the departmental landscape that accommodates a person-centric view of data, see earlier discussion in Section 8.2.1. The person-centric-view requires associating information about a person across organizations and encounters and then delivering a needs-specific view of the collated data to a DHS decision-maker based on the context of the decision being made. The OCIO and SCO have been tasked with developing recommendations on interoperable enterprise standards for the Department and DHS Privacy Office leadership will be needed to identify privacy processes that support an enterprise-level service for the person-centric-view.

8.5. Cyber Security

Secretary Chertoff identified cyber security as one of the Department's top priorities. Earlier this year, the President issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which formalized a series of efforts designed to further safeguard Federal Government systems and reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats. The Department leads the Federal effort to provide cyber security, and, given its mandate to ensure its use of technology sustains privacy protections, DHS is integrating cyber security and privacy from the start.

The Privacy Office is working together with NCSD, including the U.S. Computer Emergency Readiness Team (US-CERT), the operational arm of NCSD that serves as the national focal point for addressing cyber security issues, including analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating

incident response activities. In further support of the operational collaboration with NCSD, the Privacy Office began more strategic discussions with the recently created National Cyber Security Center (NCSC) to identify longer-range and cross-sector cyber security and privacy issues. The following summary represents some of the results of Privacy Office's work with NCSD, US-CERT, and NCSC.

8.5.1. Cyber Security Initiative Subcommittee

OMB recently established the Cyber Initiative Subcommittee of the CIO Council Privacy Committee to address the privacy issues related to all of the initiatives and enablers of the President's Comprehensive National Cyber Security Initiative (CNCI). OMB asked the DHS Chief Privacy Officer to serve as the subcommittee chair. In this role, the Chief Privacy Officer oversees the high-level interagency subcommittee, including representatives from the President's Office of Science and Technology Policy, the DOJ, OMB, the Department of Defense, and the Office of the Director of National Intelligence (ODNI).

As one of its core duties, the Cyber Initiative Subcommittee has focused on coordinating with the DHS Office of the General Counsel, US-CERT, and NCSD on drafting a model Memorandum of Agreement (MOA) between US-CERT (through DHS) and participating agencies using the EINSTEIN 2 Intrusion Detection System, which builds on its predecessor to improve computer network security for the Federal Government.

8.5.2. Cyber Security Privacy Impact Assessment

In May 2008, the DHS Privacy Office published the PIA for EINSTEIN 2, an updated version of the 2004 EINSTEIN 1 PIA. EINSTEIN 2 incorporates network Intrusion Detection System (IDS) technology into the EINSTEIN 1 framework to monitor Federal agencies' network flows for malicious activity. The EINSTEIN 2 PIA demonstrates the DHS Privacy Office's commitment to the ongoing integration of privacy protections into DHS technologies.

EINSTEIN 2 uses pre-defined signatures (patterns that correspond to known threats) from known malicious network traffic to assess potential attacks stemming from network traffic, enabling US-CERT to identify anomalous activity that might signal the unusual system behavior of an attack.

The PIA for EINSTEIN 2 details the EINSTEIN program's role to augment, not replace or reduce, current agency network security practices without impinging on privacy protections. EINSTEIN 2 contains numerous measures to address privacy concerns. In sum, the system does not seek or obtain the content of all electronic communications; rather, it scans communications during transmissions and only collects data for triggered alerts that warrant analysis. In accordance with applicable laws, the system captures flow record data that includes IP addresses but does not capture additional information that may identify the individuals communicating, unless such information is part of a security incident. Many times the analysis of this event will only require looking at the attachment and not even reviewing the contents of the email.

However, sometimes the malicious payload is hidden and delivered via the content (or body) of the email. In those circumstances, the analyst focuses on analyzing the event for the malicious payload, not on any content nor PII contained in the event. This means that the contents of the email may be viewed by a US-CERT analyst, but the focus is on the malicious activity.

If network traffic does not meet the criteria of a specific signature, however, that traffic will not be viewed by US-CERT. In addition, EINSTEIN 2 minimizes the amount of inadvertently acquired PII and strips network traffic that was captured due to a triggered alert to include only minimal non-content information, indexed by the security incident and not PII. If, by chance, the system generates a false alert, that information is deleted after review. Other security measures include keeping the EINSTEIN 2 data in a government-operated, owned, or leased secured facility operated by trained US-CERT analysts, who receive oversight, auditing, and annual privacy training. Overall, the risk associated with this network IDS is lower than the risk generated by commercially available IDS technologies because EINSTEIN 2 uses only predefined signatures, not all available signatures.

Such limitations reflect US-CERT's exclusive focus on network security. US-CERT does not have an intelligence or law enforcement mission. US-CERT will enter into a MOA with each participating Federal agency to identify clearly the roles and responsibilities of US-CERT and the participating agency. The MOAs will define clearly the protocols for information sharing that preserve privacy, and the agencies must post notices on their websites and on other major points of entry that computer security information is being collected and that the agency systems are monitored.

8.5.3. Cyber Security Training

The DHS Privacy Office conducted a privacy education and awareness training session specifically for US-CERT employees in conjunction with the rollout of the EINSTEIN 2 program. The training agenda included: an overview of the DHS Privacy Office, privacy compliance and guidance documents, and their legal underpinnings; the definition of PII; a review of PII handling guidelines and the consequences of improper handling; and the Privacy Incident Handling Guide, which covers rules and responsibilities to help in reporting and responding to incidents. This training provided the US-CERT employees with the understanding necessary to protect individual privacy and PII while conducting the cyber security work they do to protect the Nation's Internet infrastructure and coordinate defense against and responses to cyber attacks across the Nation.

8.6. National Applications Office

As described in its charter, the National Applications Office (NAO) will advocate for Intelligence Community (IC) capabilities and future technology needs to serve non-traditional users in the civil, homeland security, and law enforcement communities. The NAO "will collaborate with these potential users," the charter explains, "about IC capabilities and how and

when they might best be leveraged to support their needs in accordance with existing legal, privacy, civil rights, civil liberties, and policy requirements." The Privacy Office worked with the NAO program office to ensure privacy protections were incorporated into NAO's foundational documents and reinforced those protections in a PIA.

The NAO PIA uses the Privacy Office's articulation of the FIPPs (see Section 1) to identify potential privacy risks associated with the NAO program and to demonstrate mitigation strategies to incorporate into NAO operations.[39] As NAO develops from an office on paper into an office in practice, the Privacy Office will continue to evaluate NAO procedures to ensure it sustains embedded privacy protections in its operations, thus maintaining an ongoing collaboration.

Such collaboration was demonstrated when the Privacy Office participated actively alongside NAO to support the GAO's review of the Secretary's certification of the NAO program. Such participation offered an opportunity to exemplify the Office's focus on achieving transparency through the PIA process and the benefit of integrating privacy protections into the formative stages of DHS programs. In addition, the Privacy Office provided briefings to the Privacy and Civil Liberties Oversight Board at classified and unclassified levels, and the Chief Privacy Officer testified before Congress to offer further clarity about privacy and NAO.

9. Privacy Complaints

9.1. Internal Response Processes to Privacy Concerns

In accordance with Section 803 of the 9/11 Commission Act and OMB Memorandum 08-09, *New FISMA Reporting Requirement for FY2008*, the DHS Privacy Office has been steadily standardizing the processing, review, and reporting of privacy complaints. The DHS Privacy Office is now required to report to Congress quarterly as part of its FISMA reporting the number and types of privacy complaints received throughout the Department.

The following tables provide the figures reported to Congress and OMB covering the periods of December 1, 2007 - February 29, 2008, and March 1, 2008 - May 31, 2008. A cornerstone of the DHS complaint system is the definition of "complaints" set by OMB -- written allegations of harm or violation of privacy compliance requirements.[40] These reports reflect privacy complaints filed with the DHS Privacy Office and DHS components or programs.

[39] The NAO PIA is a program-level PIA. When NAO is used to support specific program operations, system-level PIAs will be developed to address any accompanying privacy risks. With a program-level PIA already in place, the privacy issues raised by specific IT systems can be addressed within the context of the privacy protections established for the overall NAO program.

[40] OMB-08-09

Complaints may be from U.S. Citizens and Lawful Permanent Residents as well as visitors and aliens.[41]

Privacy Complaints Received with Action Taken
(December 1, 2007 – February 29, 2008) Second Quarter

		Disposition of Compliant			
Type of Complaint	# of Complaints	Responsive Action Taken	Referred	Unable to Assist[42]	Pending
Transparency	46	1	4	0	41
Redress[43]	2,914	2,397	510	3	4
General	274	10	263	0	1
Total	3,234	2,408	777	3	46

[41] DHS Privacy Policy Guidance Memorandum 2007-01 governs mixed use systems and provides for the extension of Privacy Act protections to PII of visitors and aliens.

[42] DHS modified this category within the Q3 report to better reflect the response to the complaint.

[43] This figure includes the number of individuals who filed a redress inquiry with the DHS Traveler Redress Inquiry Program (DHS TRIP) and checked off the box on the online form that reads: "I feel my personal information has been misused." Individuals may check off one or more boxes to capture their concerns. This means that some of the 2,914 noted above may also have identified a civil rights concern, which may result in some duplication of the number of complaints reported by the DHS Privacy Office and CRCL to OMB and the Congress.

Privacy Complaints Received with Action Taken
(March 1, 2008 – May 31, 2008) Third Quarter

		Disposition of Compliant			
Type of Complaint	# of Complaints	Responsive Action Taken	Referred	No Action Required	Pending
Transparency	39	3	0	36	0
Redress[44]	630	70	17	358[45]	185
General	281	114	29	135	3
Total	950	187	46	529	188

Section 803 complaints are separated into three categories – transparency, redress, and general. As the reporting is further developed, additional categories may be added.

- *Transparency*. Complaints concerning process and procedure related to DHS activities, such as consent to receive PII, appropriate privacy notice at the time of collection, or notices provided in the *Federal Register*, such as rulemakings and SORNs.

  Example: An individual submits a complaint as part of a rulemaking that alleges the program violates privacy.

- *Redress*. Complaints concerning appropriate access, correction, and redress.

  Example: Misidentification during traveler screening at the border.[46]

[44] This figure includes the number of individuals who filed a redress inquiry with DHS TRIP and checked off the box on the online form that reads: "I feel my personal information has been misused." Individuals may check off one or more boxes to capture their concerns. This means that some of the 630 noted above may also have identified a civil rights concern, which may result in some duplication of the number of complaints reported by the DHS Privacy Office and the Office for Civil Rights and Civil Liberties to OMB and the Congress.

The number of redress complaints does not include Privacy Act requests for information or correction. In addition, the number does not include requests for correction as part of credentialing or screening programs at the Department where a redress process has been set up external to the Privacy Act process. For example, Transportation Worker Identification Credential (TWIC) has an appeal process set up to handle correction, misidentification, and other issues related to the TWIC program. Given the similarity between these redress programs and the Privacy Act process, and the fact that OMB M-08-09 specifically states that Privacy Act requests should not be included in the annual FISMA reporting, DHS has chosen not to include these numbers.

[45] DHS TRIP privacy complaints that require additional paperwork or information from the individual are considered "No Action Required" until the paperwork has been submitted. Upon submission of paperwork, the complaints will be counted as "Pending" or "Responsive Action Taken".

[46] This category excludes FOIA and Privacy Act requests for access which are reported in the Annual FOIA Report.

- *General*. Complaints related to general privacy concerns and concerns not related to Transparency or Redress.

  Example: An individual has a question about his or her driver's license or Social Security Number, which the DHS Privacy Office refers to the proper agency.

  Example: An employee's health information was disclosed to a non-supervisor.

  Example: A supervisor disclosed a personnel file to a future employer.

Complaints are also analyzed according to their disposition. These categories are responsive action taken; referred; no action required (replaces prior category of "unable to assist"), and pending.

- *Responsive Action Taken*. The DHS component or the DHS Privacy Office reviewed the complaint and a responsive action was taken. For example, an individual may provide additional information to distinguish themselves from someone else to prompt removal from a watch list.
- *Referred.* The DHS component or the DHS Privacy Office determined that the complaint would be more appropriately handled by another Federal agency or other entity and referred the complaint to the appropriate organization. This can happen when a person is stopped at a border crossing for further investigation based on a past police record.
- *No Action Required*. The DHS component or the DHS Privacy Office determined that the complaint does not ask for or require a DHS action or response. Examples are a complaint stating they are upset because of the length of wait time at an airport security checkpoint.
- *Pending.* The DHS component or the DHS Privacy Office is reviewing the complaint to determine the appropriate response.

The DHS Privacy Office will continue to upgrade and standardize its complaint processes. The DHS Privacy Office is working closely with all component Privacy Officers and PPOCs to improve identification and reporting of all privacy complaints. For example, the DHS Privacy Office plans to develop and implement a complaint handling tracking system to provide improved complaint analysis and ensure appropriate and timely responses. Further, the Office created a new position, Director of Privacy Incidents and Inquiries. Once the DHS Privacy Office has had sufficient experience with the tracking system, the Office may extend it to the components.

9.2. Responding to Public Inquiries

The DHS Privacy Office receives hundreds of email requests for information, as well as comments and complaints throughout the year. The DHS Privacy Office provides an email

address through its website at privacy@dhs.gov, which members of the public use to contact the Office. A majority of these email inquiries, however, involve issues that are outside the DHS Privacy Office's area of responsibility. When these comments, complaints, or requests are received, the requests are referred to the appropriate DHS component or other Federal agency. Examples of the emails received this year include:

- **Immigration Status** – An individual requested advice on whether a U.S. citizen can petition the State Department for legal alien status for a wife who entered the U.S. as a visitor, yet over stayed her visa. Another individual asked, "I would like to request a contact email address for inquiring and submitting information on an immigration case."
- **Citizenship and Immigration Data** – An individual stated, "I need to verify my entry and exit records. My File # is [xxxxxxxx]".
- **Watch List –** An individual wrote, "I constantly travel and each time I need to check in for Southwest, I am denied the right and ease of checking in online or in advance. I will appreciate that my identity be removed from the watch list."
- **Reduction of Use of Social Security Numbers** - An individual asked, "What can you do to reduce the unnecessary use of employee SSNs on documents where it does not appear to be essential information?"
- **PII of Foreign Nationals** – An individual asked, "I am looking for some specific direction as to the required treatment of the PII of foreign nationals, especially as it may concern the European Union."
- **Privacy Act –** An individual asked, "Why is this web site not a privacy act concern: [Email cited a URL of a website that posts name, agency, duty station, salary, and awards of Federal employees]

9.3. Relationship with the Office of Inspector General

As noted in Section 4.1 of this report, Section 802 of the 9/11 Commission Act expressly establishes formal requirements for the DHS Privacy Office to coordinate investigations of violations or abuse related to privacy within the Department with the DHS OIG. On March 23, 2008, the Chief Privacy Officer and the DHS Inspector General entered into a Memorandum of Understanding outlining the coordination efforts the two organizations would undertake consistent with the requirements of Section 802 of the 9/11 Commission Act. This includes a requirement that OIG staff members conducting privacy investigations receive adequate training on privacy laws, rules, and regulations in consultation with the Chief Privacy Officer. Section 802 requires that the OIG have an opportunity to decide whether to conduct investigations of violations or abuse. If the OIG decides against opening an investigation, it will refer to the Privacy Office for review.

In addition to the new 802 requirements, the DHS Privacy Office works closely with the OIG to ensure departmental compliance with FISMA requirements. Each year, the OIG conducts a thorough review of the Department's implementation of OMB Memorandum 07-16 privacy and security requirements. The DHS Privacy Office coordinates the response with the CISO.

10. Implementation of Privacy Guidance

10.1. Privacy Technology Implementation Guide

The *Privacy Technology Implementation Guide* (PTIG), released August 2007, is a procedural guide to help technology managers and developers integrate privacy protections into operational systems that collect, process, or produce PII. The guide offers best-practice suggestions to assimilate privacy protections and focuses on two key areas of operational IT systems — technology management, which covers managerial administration of IT systems that incorporate privacy protections, and technology development, which embodies how developers can consider privacy protections from the early stages in the system development life cycle to improve the quality and effectiveness of privacy compliance and documentation. The FIPPs form the cornerstone of the PTIG, which merges these principles with privacy compliance analysis and documentation requirements, and enables the DHS Privacy Office to "bake in" privacy protections from the beginning. By using this foundation and summarizing the stages of the privacy compliance process — initial contact and coordination, collaboration and development, reporting, and auditing — the PTIG illustrates a practical overview of privacy protection considerations to benefit technology managers and developers.

In addition to the PTIG's recommendations for IT systems in operation, it urges IT developers to use only the minimum amount of PII necessary to accomplish the system's purpose. The PTIG offers further guidance to ensure individual participation in the collection and use of PII by encouraging direct collection of PII from individuals (when appropriate) and providing individuals the opportunity for correction and redress. It also notes specific privacy considerations for internal and external information sharing, as well as the importance of data and process dictionaries and models to facilitate the analysis of how a particular system would use PII.

The PTIG models a thoughtful process of incorporating specific considerations regarding the use of PII alongside the standardized data modeling and quality assurance aspects of system development. In addition to using the PTIG and working with the Privacy Office as a general matter, IT managers and developers should begin privacy discussion early in the development life cycle with component Privacy Officers or PPOCs. The PTIG is available to DHS IT managers and developers as well as the public on the DHS Privacy Office website.[47]

[47] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_ptig.pdf

10.2. Safeguarding PII and Rules for Handling PII at DHS

During this report year, the DHS Privacy Office has drafted several new policy documents on how employees and contractors at the Department must safeguard PII, including a *Rules for Handling PII* and *Handbook for Safeguarding PII*. The DHS Privacy Office plans to issue both of these guides by early fall. The Rules will be a concise reference of how personnel must handle PII at DHS. The Handbook will provide additional explanation, resources, and instruction on how to implement these rules.

Together, these policy documents will explain why PII must be protected, how to identify and protect Sensitive PII, how to protect PII in different contexts and formats, and what to do if PII may have been compromised. The Rules and Handbook were drafted in response to the requirements of OMB Memorandum 07-16, *Safeguarding Against the Breach of Personally Identifiable Information*, and will be the basis of future training and additional guidance from the DHS Privacy Office.

10.3. Implementation of the DHS Privacy Incident Response Plan

The Privacy Office has just completed its first year of implementation of the *Privacy Incident Handling Guidance* (PIHG), the cornerstone of data breach policy within DHS. The PIHG informs DHS components, employees, and contractors of their obligation to protect the PII that they are authorized to handle and how they must respond to any suspected or confirmed potential loss or compromise of PII.[48] The PIHG defines the roles and responsibilities of personnel and management in responding to privacy incidents.

The Department has a legal obligation to safeguard PII and to implement procedures for handling both privacy and computer security incidents. The Privacy Office has the leading responsibility for implementation of the privacy incident response program throughout the Department. Through close collaboration, the DHS Chief Privacy Officer, the DHS CISO, the DHS Security Operations Center (DHS SOC) and the DHS CIO ensure that all DHS privacy and computer security incidents are identified, reported, and an appropriate response is taken to mitigate harm to DHS-maintained assets and information. While each privacy incident must be evaluated individually, the PIHG provides 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.

The PIHG strictly adheres to OMB Memorandum 07-16, which is a foundation for the management of all privacy incidents. In addition to OMB Memorandum 07-16, the PIHG also incorporates the framework for categorizing incidents described in Federal Information

[48] OMB Memorandum 06-19 requires agencies to report all suspected and confirmed incidents involving PII to US-CERT within one hour of discovering an incident. The PIHG is structured to expedite this incident reporting requirement.

Processing Standards (FIPS) 200 and NIST SP 800-53. This additional framework also necessitated amending the Concept of Operations of US-CERT to include Privacy Incident reports.

During the reporting year of July 1, 2007 – July 1, 2008, the Privacy Office made a number of updates and revisions to the PIHG and its privacy incident management program. The Privacy Office is currently updating and revising the PIHG to reflect additional OMB guidance and experience gained over this first year regarding the incidents process flows. The plan is to produce a much more succinct "tabletop" PIHG which can be used as a quick reference guide by Information System Security Managers (ISSMs), component Privacy Officers and PPOCs as well as individual information system program managers. This modified PIHG will undergo the review and approval process within DHS early this fall.

Constant communication with the DHS SOC has yielded an efficient and effective reporting system with a high level of trust between the Privacy Office and the DHS SOC analysts in charge of the incident reporting process. This close communication allows the Privacy Office to request modifications to the online reporting process when needed, as well as to obtain reporting capabilities that provide key metrics for the program.

During the reporting period, a total of 202 privacy incidents were reported to the DHS SOC. Of those, DHS investigated, mitigated, and closed 186, representing 92% of the total incidents. The following statistics detail the numbers of incidents received, the types of incidents,[49] and other metrics for the DHS Privacy Incident Management Program for this reporting period:

[49] Types of incidents are detailed in Federal Information Processing Standards (FIPS) 200 and NIST SP 800-53.

Reporting Period July 1, 2007 – July 1, 2008

Type of Incident	Number of Incidents	Percentage of Incidents
Alteration/Compromise of Information[50]	148	73%
Classified Computer Security Incident[51]	1	1%
Investigation Unconfirmed/Non-Incident[52]	15	7%
Malicious Logic[53]	2	2%
Misuse[54]	31	15%
Unauthorized Access (Intrusion)[55]	5	2%
Total	202	100%

The categories listed above describe examples of the types of incidents that may occur. Actual descriptions of incidents are not included. The majority of the reported incidents affected a small number of individuals and data. The risks associated with incidents involving laptops were mitigated due to the requirement to encrypt laptops across DHS. Mitigation and remediation of each incident is a coordinated effort between the DHS Privacy Office, DHS SOC, the PPOCs, and the ISSMs. Without this collaborative environment, DHS would not be able to respond as effectively and completely to the Privacy Incidents. When incidents indicate a need, the DHS Privacy Office has quickly and efficiently worked with these groups to implement

[50] Alteration/ Compromise of Information - The privacy incidents created and assigned to this category include a wide variety of incidents that encompass the mishandling, misdirecting, loss, or theft of PII in electronic and paper format

[51] Classified System Incident - Any security incident that involves a system used to process national security information.

[52] Investigation Unconfirmed/Non-Incident - This includes all successful unauthorized accesses and suspicious unsuccessful attempts and suspected but unconfirmed incidents.

[53] Malicious Logic - Includes active code such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges and/or information, capture passwords, and to modify audit logs to hide unauthorized activity.

[54] Misuse - A user violates Federal laws or regulations and/or Departmental policies regarding proper use of computer resources, installs unauthorized or unlicensed software, accesses resources and/or privileges that are greater than those assigned.

[55] Unauthorized Access/Intrusion - This includes all successful unauthorized accesses and suspicious unsuccessful attempts.

updated procedures to protect PII. Additionally, employees receive training regarding incidents from both their component Privacy Points of Contact as well as through the annual Culture of Privacy Awareness course on protecting all types and formats of sensitive data and the perils of sending emails with PII included (see Section 11).

Privacy incident handling has matured over the past year at DHS. The average number of open days for an incident has decreased from 54 days to 32 days during the reporting period. Consistent and cooperative management by the DHS Privacy Office, the DHS CISO, the PPOCs, the ISSMs, and the DHS SOC have all contributed to a more efficient management system.

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

On June 4, 2007, the Chief Privacy Officer issued *Privacy Policy Guidance Memorandum 2007-02 Regarding Use of Social Security Numbers at the Department of Homeland Security*. Based on policies communicated in this memorandum, the DHS Privacy Office inventoried all existing systems that use and collect SSNs and made a determination of whether the system: (1) needed SSNs to carry out a DHS mission-related function, and (2) required the SSN by statute, regulation, and/or pursuant to a specific authorized purpose. As part of this process, the DHS Privacy Office also asked system owners to validate that systems using SSNs properly secure that information with encryption and restricted availability.

The DHS Privacy Office conducted a review of all systems that collect or use SSNs at DHS as part of its ongoing effort to eliminate unnecessary collection and use of SSNs. This review was conducted in response to OMB Memorandum 07-16 requirement that agencies review and reduce unnecessary uses of SSNs. Results of the review revealed that the majority of DHS systems using SSNs are necessary and authorized. Fewer than ten (10) instances were identified as unnecessary, and the DHS Privacy Office worked with component Privacy Officers and system owners to eliminate those unnecessary uses. Below are some examples of how SSNs were eliminated from systems:

- For a system that processed FOIA and Privacy Act requests from the public, the component added language on the request form advising that SSNs not be sent by requestor, and introduced a process to redact any SSNs on forms before scanning and uploading forms into the system.
- For a system that used employee's SSNs as the system unique identifier, the system owner assigned each file a replacement nine-digit number beginning with 8, which is not an SSN format, to replace SSN as system identifier.
- Some systems used the last four digits of a person's SSN as a PIN or access code. System owners replaced the last four digits of SSN with the person's four digit month and day of birth.

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

The DHS policy regarding privacy protections afforded to non-U.S. persons for information collected, used, retained, and/or disseminated by the Department of Homeland Security in so-called "mixed systems," i.e., those systems that contain information on both U.S. and non-U.S. persons, is set forth in the DHS Privacy Office memorandum *Privacy Policy Guidance Memorandum Number 2007-1 ("Mixed Use Policy")*, issued on January 19, 2007. As a matter of law, the Privacy Act provides statutory privacy rights to U.S. citizens and Legal Permanent Residents (LPRs), but does not cover visitors or aliens. As a matter of DHS policy, any PII collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as if it were subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien. Under this policy, DHS components handle non-U.S. person PII held in mixed systems in accordance with the FIPPs, as set forth in the Privacy Act. For example, under TRIP, non-U.S. persons have the right of access to their PII and the opportunity to amend their records, absent an exemption under the Privacy Act.

Two DHS systems, launched or modified during the reporting period, demonstrate how this policy has been implemented: the Electronic System for Travel Authorization (ESTA) and the Automated Targeting System (ATS). The ESTA and ATS SORNs explain that DHS policy allows persons, including foreign nationals, to seek redress through DHS TRIP. For example, individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by a DHS component may submit a redress request through DHS TRIP. The program provides a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs, such as airports and train stations, or when crossing U.S. borders. TRIP also provides a means for travelers to correct erroneous information stored in DHS databases through one application.

11. Internal Education and Training

The DHS Privacy Office continued to expand its training portfolio to improve employee recognition and understanding of the privacy concerns that may occur within the course of their daily duties and responsibilities. DHS employees, including contractors, must have the knowledge and tools to handle and protect PII in a responsible and appropriate manner. In addition to providing mandatory training, the DHS Privacy Office has conducted a number of targeted supplemental training courses to further infuse privacy into the Department's activities. Further, the Office created a new position, an Associate Director of Privacy Policy and Education, which is intended to increase the Office's capacity to conduct training. The sections that follow describe these mandatory and supplemental training courses.

11.1. Mandatory Training

The Privacy Act and OMB Circular A-130 mandate regular and annual Privacy Act training for employees and contractors. The DHS Privacy Office provides introductory privacy awareness training to all new DHS headquarters employees on a bi-weekly schedule as part of the new employee orientation session.

Beginning in April 2008, a series of privacy-related slides were included in the *Security Tuesday* Security Awareness training required for all new employees and contractors. This training supplements the *Culture of Privacy Awareness* training the DHS Privacy Office conducts with the assistance of the PPOCs. In addition to the information technology security mandates, *Security Tuesday* training provides the newly added privacy training slides, which focus on protection of PII on IT systems and mobile devices and basic privacy incident handling procedures. This training is conducted in close coordination with the CISO.

The *Culture of Privacy Awareness* training expands on the basic concepts presented in the new employee orientation to provide an understanding of the essentials of the Privacy Act and E-Government Act, including individual responsibility to use PII only for authorized purposes and to protect it from loss. A number of components have incorporated this course into their own training programs. It will also be a featured course on the DHScovery, a new web-based Learning Management System for DHS Headquarters employees, starting in fall 2008. In addition, the DHS Privacy Office has shared this training course with other Federal agencies, including the Office of Personnel Management, State Department, Department of the Navy, Department of the Treasury, and Department of the Interior. This class will be mandatory in FY 2009.

11.2. Expanding Awareness through Supplemental Training

During the past year, the DHS Privacy Office developed *Privacy Act 101* and *Privacy Act 201* to supplement the required training courses. These interactive training programs are available on compact discs for distribution to all components and Headquarters Offices. The DHS Privacy Office is working with DHScovery to also make these available on the online platform later this year.

Privacy Act 101 provides employees and contractors with the essentials concerning the Privacy Act, including a basic understanding of what is PII; what is a system of records; when is a SORN required; how can information be collected, used, maintained, or disseminated in compliance with the Privacy Act; and other related topics. Further, it introduces DHS employees and contractors to the FIPPs. The course addresses employee and contractor responsibilities, as well as consequences for non-compliance and violations of the Privacy Act.

Privacy Act 201 is intended for program managers, developer team leads, PPOCs, and Department supervisors to instruct on management responsibilities concerning the Privacy Act. *Privacy Act 201* also includes refresher information from the *Privacy Act 101* course. The DHS

Privacy Office is working with the DHS Office for Advanced Learning Directives to make both *Privacy Act 101* and *Privacy Act 201* available through the DHScovery learning management system.

In addition to the courses listed above, the DHS Privacy Office participates in *DHS 101* training, which is held quarterly for DHS employees seeking an overview of all DHS components' roles and activities. The Department is developing a web-based version of this department-wide program, which will include an overview of the responsibilities and role of the DHS Privacy Office.

The DHS Privacy Office also conducts quarterly PIA and SORN workshops for all DHS employees and contractors responsible for drafting these compliance documents within the components. The hands-on training details the PIA development and review process and provides an interactive forum for attendees responsible for drafting PIAs and SORNs.

11.3. Privacy as Part of Security Training

As mentioned in Section 11.1, privacy training is also part of the *Security Tuesday* required training. Additionally, every August, the DHS Privacy Office participates in the DHS Annual Security Awareness Training conference sponsored by the CISO. This conference brings together over 3,000 information technology and security professionals from throughout DHS. At the 2007 event, the DHS Privacy Office conducted a number of sessions focusing on PIA, PTA, and incident response training.

11.4. DHS Privacy Office Staff Training and Certification

In addition to training others, the DHS Privacy Office seeks to educate its own staff to maintain a high level of awareness of the developments in privacy law and policy. Consequently, DHS Privacy Office staff participates at national conferences and attends specialized training programs.

Additionally, all DHS Privacy Office staff has been required to obtain the Certified Information Privacy Professional/Government (CIPP/G) certification offered by the International Association of Privacy Professionals (IAPP). In order to be recognized by the IAPP as a CIPP/G, privacy professionals must pass both the Foundation and CIPP/G examinations.[56] DHS Privacy Office staff also regularly attend conferences put on by the American Society of Access Professionals (ASAP) conferences and workshops.

[56] The DHS Privacy Office is concerned that IAPP is primarily an organization for commercial or private sector privacy professionals and does not provide sufficient content for public sector privacy professionals, beyond the Foundation and CIPP/G training and certification, which in 2008 cost $740 (Foundation training and examination) and $255 (CIPP/G training and examination), respectively. DHS Privacy Office staff has been working with IAPP to improve and expand their focus to include more public sector privacy issues and speakers.

A significant change for the office has been its work on intelligence community issues. The Privacy Office anticipates increased demands in this area, with a view towards building in-house expertise to understand related challenges. Senior staff took several advanced courses on intelligence and information operations law and policy offered by the U.S. Army Judge Advocate's School in Charlottesville, Virginia.

The Privacy Office also has reached out to members of the intelligence community to better understand the community and its approach to Executive Order 12333, the Privacy Act, and FOIA. The Privacy Office has learned much from I&A and ODNI, as well as several Department of Defense intelligence activities and these relationships will benefit the Privacy Office in the future. Unfortunately, the Privacy Office's outreach efforts have not always been successful. After months of coordinating with the Central Intelligence Agency (CIA) to attend the CIA's FOIA and Privacy Act training to better understand how to handle FOIA requests in an intelligence context, Privacy Office staff were denied the opportunity to attend because of clearance issues at the CIA.

11.5. Additional DHS Privacy Training

The DHS Privacy Office also conducted specialized training for a number of programs, including staff of US-CERT and I&A. DHS Privacy Office staff provided in-person training tailored to the issues most relevant to these programs. In addition to the training programs offered by the DHS Privacy Office, a number of the component Privacy Officers and PPOCs developed creative privacy training programs for their staff. For example, the USCG conducted an All Hands Training and Privacy Awareness week for USCG members and employees (see Section 3.5). S&T held Privacy Awareness Day, including multiple one hour sessions on protecting privacy (see Section 3.3.2). Finally, the TSA Transportation Security Administration designed a poster campaign promoting protection of PII (see Section 3.4.2).

11.6. Reporting Training Activities to Congress

The DHS Privacy Office now reports quarterly to Congress about its training activities in accordance with Section 803 of the 9/11 Commission Act. These statistics reflect the privacy training conducted by the DHS Privacy Office and the components. The figures below combine the March and June 2008 reports and cover the period of December 1, 2007, through May 31, 2008:

- DHS personnel and contractors took classroom-based privacy training courses in 3,777 instances.

- DHS personnel and contractors took computer-assisted privacy training courses in 59,401 instances.[57]

12. Outreach

12.1. Congress

During this reporting period, the DHS Chief Privacy Officer appeared three times before Congressional Committees and Subcommittees. Each of these hearings is described below.

On September 6, 2007, Mr. Teufel appeared before the House Committee on Homeland Security to address the DHS Privacy Office's efforts to preserve privacy within the NAO, a newly formed program within I&A. During his testimony, the Chief Privacy Officer reviewed the findings of the PIA conducted by DHS Privacy Office in coordination with the NAO leadership and staff, and described the role his office plays in the NAO governance structure. In addition, Mr. Teufel promised the Committee that the DHS Privacy Office "will be vigilant in our oversight responsibilities to ensure continued compliance with privacy law and Federal policies regarding the collection, use, maintenance, and dissemination of records" within the NAO.

On March 11, 2008, Mr. Teufel was invited to testify before the House Committee on Oversight and Government Reform, Subcommittee on Information Policy, Census, and National Archives. The hearing was entitled "Privacy: The Use of Commercial Information Resellers by Federal Agencies." Acknowledging that "Government use of commercial data aggregators may pose particular privacy concerns," the Chief Privacy Officer highlighted the steps the DHS Privacy Office has taken to understand the risks and mitigate the effects such use has on individual privacy. These included a public workshop focusing on the use of commercial data and two reports on the subject authored by the DHS Privacy Office's advisory committee, the DPIAC. Consistent with one of the recommendations of the DPIAC, the Chief Privacy Officer explained how PIAs are a critical tool to examine how programs utilizing commercial data preserve privacy by adhering to the FIPPs.

Mr. Teufel made his first appearance before a Senate Committee on June 18, 2008, testifying at a hearing held by the Senate Homeland Security and Governmental Affairs Committee. He sat on a panel with the GAO Director of Information Management, who introduced a report on the coverage of Federal privacy law. Before Congress adopts any changes to either the Privacy Act or E-Government Act, the Chief Privacy Officer urged members to understand that the consequences could be "far-reaching," and that changes should be made only following "deliberate consider[ation]." The Chief Privacy Officer ended his comments by

[57] DHS offers multiple computer training courses. An individual may have taken multiple courses if their current job requires such training. This number includes annual privacy awareness training for the US Coast Guard and ICE.

offering the DHS Privacy Office's assistance in understanding those consequences should Congress or the White House wish to amend existing Federal privacy laws. During the reporting period, the Office also provided several briefings to Congressional committee staff and responded to follow-on questions. Staff provided briefings on topics such as NAO, international information sharing, and new SORNs.

12.2. Communication with the Public and the Privacy Advocacy Community

Throughout the year, the DHS Privacy Office engaged in a wide variety of efforts to inform the public of privacy matters at the Department and to solicit concerns and expertise from a number of experts within the privacy advocacy community as well as from academic, think tank, and other policy experts. The Chief Privacy Officer conducted an active outreach effort with numerous speaking engagements throughout the year. The events were geared to educate industry, professional associations, policy makers, and the public about the perspective of the DHS Privacy Office on such privacy issues as cyber security, biometrics, identity management, identity theft, data security, international privacy, and other important privacy topics. Throughout the year, the Chief Privacy Officer and senior Privacy Office staff attended numerous public conferences, here and abroad, to discuss the work of the Office and to engage in discussions with others regarding key privacy issues. The international events are noted in Section 16. These engagements cover a wide diversity of topics and provide an opportunity to educate the public about how the Privacy Office is addressing privacy at the Department and, in return, an opportunity to learn about new developments in the privacy and security arena.

Some of the topics covered at these events include biometrics, RFID, identity theft, CCTV, fusion centers, data breaches, and cyber security. Examples of these events during 2008 include the following:

- Johns Hopkins University, *Radio Frequency Identification Security Workshop: From Theory to Practice* (Baltimore, MD, January 2008)
- Electronic Privacy Information Center's *14th Annual Privacy Coalition Event* (Washington, DC, January 2008)
- *Data Privacy In Transatlantic Perspective: Conflict or Cooperation?* (Duke University School of Law Raleigh-Durham, North Carolina, January 2008)
- The 9th Annual Privacy and Security Conference: *Digital Dilemmas, Digital Dreams: Privacy Security and Society in New World Networks.* (Victoria, British Columbia, February 2008)
- Institute for Defense and Government Advancement's *Biometrics for National Security and Defense Conference* (Arlington, VA, February 2008)
- International Association of Chiefs of Police, *Technology and Policy Symposium, CCTV: Gaining Public Support and Protecting Privacy* (San Diego, February 2008)

- American Society of Access Professionals 1st National Training Conference (Lake Buena Vista, Florida, March 2008)
- AFCEA International Solutions Conference *Privacy Concerns in a Collaborative Environment* (Washington, DC, March 2008)
- The 2008 National Fusion Center Conference in (San Francisco, CA, March 2008)
- Global Consortium Conference Department of Defense Intelligence Community Financial Sector Forum (New York City, April 2008)
- RSA Conference, panel: *Your Agency Had a Data Breach! What Do You Do?* (San Francisco, CA, April 2008)
- The 7th International Public Safety/Counterterrorism Conference, panel: *Border Security vs. Personal Privacy – The Advantages of Collaboration* (Seattle, WA, April 2008)
- ID Analytics, Inc., Identity 2008 Conference, panel: *Privacy In The Age of Analytics* (Carlsbad, California, May 2008)
- The 18th Annual CTST (formerly CardTech SecurTech) 2008 Conference (Orlando, FL, May 2008)
- The Second Annual American Bar Association's National Institute Cyberlaw: Expanding the Horizons panel: Criminal Aspects of Identity Theft: Financial Records, Data Mining, and Online Threats (Washington, DC, June 2008)
- Advanced Learning Institute's Biometrics for Government Conference, panel: *How To Deploy And Coordinate Identity Technologies To Maximize Results And Achieve Objectives* (Washington, DC, July 2008)

Outreach to the privacy advocacy community is a high priority of the DHS Privacy Office. During this report period, the Chief Privacy Officer and senior members of the Office met with members of the privacy community to inform them of activities of the Office, as well as to learn about any concerns they had regarding departmental activities. This outreach has led to a close working relationship that enables the privacy community to feel that it can reach out to the DHS Privacy Office with questions and comments at anytime and that their views are respected and will be voiced within the Department. Among the issues they raised during this year were the cyber security initiative, REAL ID, RFID, EDLs, NAO, lap top searches, fusion centers, DHS TRIP, Passenger Name Records, and international data sharing.

12.3. Workshops

To further educate itself, government employees, and the public, the DHS Privacy Office holds several workshops annually to discuss issues within the privacy community and provide

insight to others regarding the privacy practices implemented within DHS. The DHS Privacy Office held three privacy workshops this year; *Privacy Compliance Fundamentals - PTAs, PIAs, and SORNs*, *CCTV: Developing Privacy Best Practices*, and *Implementing Privacy Protections in Government Data Mining*. The descriptions of these workshops were published in the *Federal Register* and can be found by accessing the DHS Privacy Office website.[58]

12.3.1. Compliance Workshops

On May 23, 2008, the DHS Privacy Office held a workshop, *Privacy Compliance Fundamentals - PTAs, PIAs, and SORNs* to provide in-depth training on the privacy compliance processes at DHS. The workshop specifically illustrated the steps to write PIAs and SORNs by using a case-study to exemplify the systematic process of writing each.

12.3.2. Closed Circuit Television

On December 17-18, 2007, the DHS Privacy Office held a public workshop, *CCTV: Developing Privacy Best Practices*, which brought together leading government, academic, policy and international experts to discuss the impact on privacy and civil liberties of CCTV and possible best practice principles for its use. The workshop examined how technology, local and international communities, law enforcement, government agencies, and privacy advocates can shape the use of CCTV and what safeguards should be in place as the use of CCTV expands. The workshop served as a valuable resource to the DHS Privacy Office in its joint effort with CRCL to develop a best practices guide for government use of CCTV. The DHS Privacy Office, in conjunction with CRCL, is finalizing its report on the workshop and proposed best practices for government agencies implementing CCTV programs. This initiative is in its final stages and will be released later this year.

12.3.3. Data Mining

On July 24-25, 2008, the DHS Privacy Office held a public workshop entitled *Implementing Privacy Protections in Government Data Mining.* The public workshop brought together leading academic, policy, and technology experts to discuss the actual and potential impacts of government data mining on individuals and on society. Participants also explored methods of validating the accuracy and effectiveness of data mining models and rules, and the role of anonymization tools and automated audit controls in protecting privacy. The final panel discussed development of best practices principles to guide DHS data mining research and activities in support of the Department's mission. The DHS Privacy Office is now working with S&T to develop a set of data mining research principles to build privacy protections into its research projects, including those that involve data mining research.

[58] http://www.dhs.gov/xinfoshare/committees/editorial_0699.shtm

12.4. DHS Speaker Series

During this reporting period, the Privacy Office initiated a speaker series. This series is intended to bring industry experts to DHS in an effort to highlight privacy topics of interest. This provides the DHS staff an opportunity to discuss privacy issues in an informal setting with privacy experts. The first speaker was Professor Daniel Solove, author of *Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press 2007). Professor Solove spoke in June 2008 on the topic of "Understanding Privacy." Future programs are planned during the next reporting period.

12.5. Privacy Matters

Since 2005, the DHS Privacy Office has produced a newsletter entitled, *Privacy Matters*, to inform our DHS colleagues, Members of Congress, our international partners, and the privacy community at-large of the important work of the Office. The newsletter is available in hard copy. Given the newsletter's broad audience, *Privacy Matters* is an important part of the DHS Privacy Office's outreach program.

Topics featured in Privacy Matters over the fall 2007 and spring 2008 include:

- Highlights of DPIAC meetings;
- International Outreach;
- Privacy Office news, including new staff members and initiatives;
- PIA, CCTV, and Data Privacy Tutorial Workshops;
- Legacy SORN project; and
- Promoting privacy protections through Chief Privacy Officer outreach.

12.6. Web Outreach

The Office actively maintains a webpage that provides a wealth of information regarding the activities of the Office. The webpage is available at www.dhs.gov/privacy. The site includes materials such as: authorities; reports; workshop agendas, reports, and transcripts; DPIAC materials; Management Directives and guidance; and privacy compliance documents, including the latest PIAs and SORNs.

This reporting period also marked the Chief Privacy Officer's first entries on the Department's Leadership Journal.[59] Essentially in the form of a web log ("blog"), the Chief Privacy Officer made entries on topics such as the previous DHS Privacy Office Annual Report

[59] The DHS Leadership Journal is available on the internet at www.dhs.gov/journal/leadership.

to Congress, as well as the benefits of approaching privacy and security together, versus making choices to "balance" between the two. This has been an effective outreach tool that allows the Office to quickly present its views to a large audience.

13. Interagency Contributions to Privacy

13.1. Information Sharing Environment

The Information Sharing Environment (ISE) was mandated in December 2004 with the enactment of IRTPA. On December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies regarding *Guidelines and Requirements in Support of the Information Sharing Environment*, which specified tasks, deadlines, and assignments necessary to further the ISE's development and implementation.

The Memorandum directed that the ISE leverage ongoing information sharing efforts in the development of the ISE. The assignments included five guidelines, as follows:

- Define common standards for how information is acquired, accessed, shared, and used within the ISE;
- Develop a common framework for the sharing of information between and among executive departments and agencies and state, local, and tribal governments, law enforcement agencies, and the private sector;
- Standardize procedures for sensitive but unclassified information;
- Facilitate information sharing between executive departments and agencies and foreign partners; and
- Protect the information privacy and other legal rights of Americans.

The Memorandum also directed agencies to promote a culture of information sharing and to assist the Director of National Intelligence and the PM-ISE in implementing the President's memorandum. Subsequently, the 9/11 Commission Act expanded key provisions of IRTPA and provided additional guidance to the ISE, as well as expanded the definition of terrorism information to include weapons of mass destruction.

The DHS Privacy Office supports the implementation of the ISE in many ways. Within the Department, members of the DHS Privacy Office staff participate in the Information Sharing Coordination Council, which provides guidance to Departmental leadership on information sharing issues, including issues related to privacy. The Chief Privacy Officer, moreover, sits as a non-voting member on the Department's senior-level Information Sharing Governance Board. This board is responsible for overseeing the vast portfolio of DHS information sharing programs. The Chief Privacy Officer's presence ensures privacy is considered throughout the development cycle of any information sharing arrangement undertaken by the Department.

The Chief Privacy Officer also contributes to the National effort to establish information sharing policies which are sensitive to privacy rights. For instance, he is a member of the PM-ISE's Privacy Guidelines Committee (PGC), an interagency effort formed in order to implement Presidential Guideline 5, to protect the privacy and other legal rights of Americans. In addition, members of the DHS Privacy Office staff assisted the work of the PGC in many ways, including serving as a co-chair of its State and Local Working Group (SLWG).

During the reporting year, and with the support of the Chief Privacy Officer, the PCG issued its *Privacy Guidelines for the Information Sharing Environment*, as well a number of resources ISE participants can employ to meet their privacy requirements. The SLWG worked hard to translate the ISE requirements into materials which non-Federal participants—particularly fusion centers—can use to meet the requirement that they develop privacy policies "at least as comprehensive" as Federal ISE members. In November 2007, a DHS Privacy Office staff member represented the ISE at the Southeast Regional Fusion Conference in Savannah, Georgia, hosted by DOJ's Bureau of Justice Assistance. At the Conference, the DHS Privacy Office employee delivered a presentation entitled *The Importance of Privacy in the Information Sharing Environment*, and helped introduce a Privacy Policy Workbook participants could use to develop their own written privacy policies.

During the coming reporting year, the DHS Privacy Office will turn its attention to identifying, assessing, and documenting the Department's ISE-compliant privacy policy. These policies aid in preserving privacy whenever homeland security is shared by members of the ISE.

Within the Department, the Privacy Office will ensure the DHS Information Sharing Strategy is deployed in manner that respects individual privacy interests and implements the FIPPs. The Privacy Office will continue its close engagement with CRCL to draft the Department's Privacy and Civil Liberties Policies, according to ISE requirements.

The Privacy Office will continue to work with State and local fusion centers as they respond to newly issued ISE guidelines. In particular, the Privacy Office anticipates working with all fusion centers and the PM-ISE to craft rules governing the use of Suspicious Activity Reports, a common law enforcement tool which may present unique privacy challenges as it becomes part of ISE covered information. Finally, together with DOJ and the PM-ISE, the Privacy Office and CRCL will roll out the training developed for State and local fusion center representatives, and described in Section 5, above. More information about the ISE may be found at www.ise.gov.

13.2. Chief Information Officers Council's Privacy Committee

The DHS Privacy Office participates actively on the interagency CIO Council's Privacy Committee, formerly the OMB Privacy Committee. This interagency committee includes the Senior Agency Official for Privacy from all Federal agencies and provides an important forum to address cross agency privacy issues. This past year, the Committee, which meets at least

quarterly, focused on implementation of OMB Memorandum 07-16 and the 9/11 Commission Act. The DHS Privacy Office co-chairs the planning committee for the first Federal Privacy Summit, scheduled for October 23, 2008, to strengthen training across the Federal Government for Federal employees working on privacy matters. The Privacy Summit will be held in conjunction with the CIO Council's annual Federal IT Summit.

14. Data Privacy and Integrity Advisory Committee

The DPIAC operates under the authority of the Federal Advisory Committee Act (FACA) (5 U.S.C. App) to advise the Secretary of Homeland Security and Chief Privacy Officer on issues relating to programmatic, policy, operational, administrative, and technological issues within the DHS that affect individual privacy, data integrity and other privacy-related matters. Members serve as special government employees and represent a balance of relevant opinions on privacy from the private sector, academia, and the privacy advocacy community.

During the reporting period, Secretary Chertoff asked the Chair and Vice Chair to continue their service for a second one-year term, and reappointed five members to serve additional three-year terms. One individual was selected to fill the remaining time of a member who resigned.

On March 25, 2008, the Department filed a new DPIAC charter with the General Services Administration (GSA), which has administrative responsibilities under FACA. The new charter made four substantive changes:

- Authorized appointment of up to three ex officio members from the ranks of DHS component Privacy Officers.
- Required the committee to examine tasks submitted in writing by the Secretary of Homeland Security, the Chief Privacy Officer, or the Designated Federal Official.
- Unified membership terms of the SGE members to three years.
- Required at least one meeting per year.

The charter and other information about the DPIAC are available on the GSA website, www.gsa.gov.

The DHS Privacy Office generally holds quarterly DPIAC meetings, however, due to a series of continuing resolutions, the Privacy Office called only three public meetings during this reporting period. Each meeting is described in the paragraphs that follow.

On September 17, 2007, the DPIAC held a public meeting in Arlington, Virginia. The Deputy Chief Privacy Officer opened the meeting with an update of the DHS Privacy Office's significant activities since the last meeting. The Committee heard testimony from the Hon. Charles Allen, DHS Under Secretary for Intelligence and Analysis about the Department's

program to interact with State and local fusion centers. Members also heard panels on fusion centers both from program participants and the privacy advocacy community. The meeting concluded with an update from the US-VISIT Privacy Officer of the US-VISIT program within USCIS.

The March 12, 2008, DPIAC meeting was held in El Paso, Texas. The Deputy Chief Privacy Officer welcomed the committee and updated the members on recent activities of the DHS Privacy Office. The Committee heard DHS and advocacy testimony on DHS' E-Verify program, managed by DHS within CIS. In addition, the committee benefited from the perspectives offered by residents of the State of Arizona, which has widely implemented the E-Verify program. The TSA Privacy Officer concluded the meeting with an update of TSA's recent privacy compliance program.

During the trip, DPIAC members had an opportunity to tour a wide range of DHS operations at the United States southern border with Mexico, including truck, car, and pedestrian crossing inspections; ICE detention operations; Immigration Court proceedings; U.S. Border Patrol monitoring at the border; and in-processing of individuals suspected of being in the United States unlawfully. The Committee also toured the El Paso Intelligence Center, a multi-party intelligence fusion center.

The third meeting during the reporting period was held on June 11, 2008, in Arlington, Virginia. Once again, the Deputy Chief Privacy Officer welcomed the committee and provided the DHS Privacy Office update. The Committee heard from the Hon. Daniel W. Sutherland, Officer for Civil Rights and Civil Liberties at DHS. Mr. Sutherland discussed his office's efforts to embed respect for civil rights and liberties into DHS programs, and introduced the new tool created by his office to analyze civil liberties issues: the Civil Liberties Impact Assessment (CLIA). Mr. Sutherland also briefly outlined his vision for the Privacy and Civil Liberties Oversight Board, for which he has been nominated by the President to Chair. Mr. Sutherland's remarks were followed by a panel exploring the CLIA in more depth, comprised of a representative from his office, the Deputy Civil Liberties Protection Officer Office at ODNI, and a representative from the Constitution Project, and an organization that provided CRCL with valuable feedback when they were developing the CLIA tool.

The Committee also heard a government panel on the E-Verify program, following their request for more information after the March 12 meeting, and two panels regarding the ISE. The first ISE panel presented government perspectives, focusing on the recently released *National Strategy for Information Sharing* and the *DHS Information Sharing Strategy*. The second ISE panel provided a privacy advocacy perspective on some of the challenges faced with implementing an information sharing environment.

The DHS Privacy Office maintains a DPIAC page on its public website with extensive information about the committee, including meeting agendas and minutes, membership information, and reports and recommendations and archives of past meetings.[60]

15. Data Integrity Board

The Chief Privacy Officer serves as the Chairman of the DHS Data Integrity Board (DIB). This body is responsible for approving and overseeing the use of computer matching programs by the Department, under the *Computer Matching and Privacy Protection Act of 1988*, which amended the Privacy Act (5 U.S.C. 552a).

With certain exceptions, a "matching program" is "any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs…"[61]

Before the Department can match its data with another Federal or State government, either as the recipient or the source of the data, it must enter into a written Computer Matching Agreement (CMA) with the other party, which must be approved by the DHS DIB. Each CMA must include a description of:

- The purpose and legal authority for conducting the program;
- The justification for the program and the anticipated results, including a specific estimate of any savings;
- A description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;
- Procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency;
- Procedures for verifying information produced in such matching program;
- Procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;

[60] http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm

[61] 5 U.S.C. 552a(a)(8)(i)(1).

- Procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;
- Prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;
- Procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;
- Information on assessments that have been made on the accuracy of the records that will be used in such matching program; and
- That the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

During the reporting year, DHS entered into one CMA with the Department of Education (ED), reauthorizing an existing matching program. Under the agreement, ED may utilize records within a system held by USCIS to confirm the immigration status of alien applicants for, or recipients of, a number of financial aid programs administered by ED. The DHS DIB approved this CMA unanimously. [62]

16. International Privacy Policy

The DHS Privacy Office International Privacy Policy (IPP) group promotes international cooperation and understanding of privacy issues relevant to the Department's mission and operations. The Office educates the international community about DHS privacy practices and engages in dialogue through multilateral and bilateral partnerships. The Office provides counsel within the Department and to other agency partners on existing and emerging changes in privacy practices and global policy approaches, and provides advice to the Department and U.S. delegations negotiating international agreements related to personal information collection and sharing.

16.1. Advisor on International Affairs

The DHS Privacy Office supports the Policy Office and DHS components engaged in international activities. Many of the Department's cross-border efforts involve information sharing with foreign governments and regional organizations. The DHS Privacy Office

[62] Notice of this CMA is available on the Federal Register at 72 FR 53235-53236 (September 18, 2007).

contributes expertise in the planning stages of international information sharing arrangements with foreign partners, as well as in the negotiations and oversight of resulting agreements. The DHS Privacy Office also serves as a resource to U.S. Government agencies involved in cross-border information sharing arrangements.

The DHS Privacy Office participated in the following initiatives during this reporting period:

- *Agreement with Germany on Enhancing Cooperation in Preventing and Combating Serious Crime.* The DHS Privacy Office provided support to the DHS Policy Office to finalize this agreement between the U.S. and Germany. The 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.

- *Agreement between the U.S. and the EU on the Passenger Name Records (PNR).* The U.S. – EU PNR agreement was signed in July 2007. The DHS Privacy Office was an important resource to the DHS negotiating team and continues to provide the Department, privacy advocates, and international parties with supporting information regarding its implementation. A joint review with the European Commission is expected to begin before the end of 2008. The DHS Privacy Office remains intimately involved in ensuring DHS adheres to its commitments as spelled out in this agreement, and will monitor EU reciprocity upon implementation of a proposed EU PNR plan.

- *Memorandum of Understanding between the Canada Border Services Agency and U.S. Customs and Border Protection Regarding the Use, Disclosure and Storage of Canadian Enhanced Driver's Licence Information.* The DHS Privacy Office provided oversight and comments to this agreement, signed in March 2008.

- *High Level Contact Group (HLCG).* Following Ministerial discussions in November 2006, an informal, high level advisory group was created to discuss privacy in the context of information exchanges for law enforcement purposes as part of a wider reflection between the U.S. and EU on how best to prevent and fight terrorism and serious transnational crime within the privacy parameters of each jurisdiction. The DHS principals for this group are the Assistant Secretary for Policy and the Chief Privacy Officer. The group is also composed of senior officials from the U.S. Departments of Justice and State, as well as the European Council Presidency and European Commission. The goal of the HLCG is to explore ways that enable the U.S. and EU to work more closely and efficiently together in the exchange of law enforcement information while ensuring privacy remains protected. The group has identified several "common principles" of an effective regime for privacy protection

as the first step towards that goal. The HLCG continues to discuss the remaining principles and the nature of a final agreement.

- *Memorandum of Understanding with UKVisas Regarding Information Vetting and Sharing*. The DHS Privacy Office reviewed this MOU with the US-VISIT Privacy Officer to ensure privacy protections were included in the text, which provides for collection of biometric and biographical information by USCIS for forward transfer to the UK in support of the adjudication of applications for visas to the UK. The DHS Privacy Office also reviewed the PIA for this program.

16.2. Working with the International Community

The Office represents the Department in the international privacy community. One of the DHS Privacy Office's primary goals is to promote understanding of how privacy issues are relevant to the Department's mission and operations. The FIPPs, first codified in the Privacy Act and later as the OECD Privacy Guidelines, are the basis for the privacy legislation of most countries. DHS promotes confidence in its programs by demonstrating how these shared FIPPs are incorporated into DHS systems and policies. DHS also promotes reciprocity as an underlying principle for fostering the trust necessary for sharing vital information with ease, security, and transparency. This year, the DHS Privacy Office endeavored to strengthen existing affiliations and cultivate new partnerships in Europe, Asia, and the Americas. For example, the Department is planning exchanges with Data Protection Authorities from Spain, the UK and other European countries. The subsections below describe the Department's international activities during the reporting period.

16.2.1. Europe

The DHS Privacy Office remained actively engaged with the European Union (EU) and data protection authorities of several EU Member States. The Office is in regular contact with the EU Presidency, European Commission, European Parliament members, and Member State Data Protection Authorities. During this reporting period, the DHS Privacy Office met with numerous European privacy and security officials in the U.S. and abroad, including:

- Officials representing the European Commission;
- The Chair of the European Commission's Article 29 Working Party;
- The European Data Protection Supervisor;
- Data protection officials from Austria, Belgium, Spain, Portugal, France, Germany, the Netherlands, Ireland, and the United Kingdom (UK); and
- Parliamentarians from the EU, the UK, and Germany.

The Chief Privacy Officer and Deputy Chief Privacy Officer spoke at several events with European audiences, such as the American and International Associations of Airport Executives'

conference in Vienna, Austria, and the German American Lawyers Association in Washington. The Chief Privacy Officer also spoke at the European Commission's Conference on Public Security, Privacy and Technology in Brussels, Belgium, where he introduced the idea of transparency as a privacy safeguard in security programs, as practiced by the Department.

The Privacy Office was also pleased to host Phil Jones, Assistant Commissioner for the UK's Information Commissioner's Office, at the Privacy Office's CCTV workshop. Mr. Jones spoke about the growing use of CCTVs in the UK and the ICO's recently updated Code of Practice to improve compliance with the UK's data protection legislation.

16.2.2. Asia

The DHS Privacy Office engaged the Asian privacy community primarily through support of the Asia Pacific Economic Cooperation (APEC) Privacy Framework. The DHS Privacy Office encourages implementation of these common, FIPPs-based principles as a way to protect privacy without impediment to cross-border data flows. Throughout the reporting year, the DHS Privacy Office participated as part of the U.S. Government's delegation before the APEC Electronic Commerce Steering Group and Data Privacy Subgroup to discuss cross-border privacy rules and projects, and contributed to U.S. interagency positions with DHS interests.

The Office is in regular contact with privacy authorities in New Zealand and Australia, and closely monitors the development of privacy legislation and policy throughout the region. Australia underwent an extensive review of its existing privacy legislation this year, which offered several opportunities for discussion of best practices and lessons learned. Like the U.S., Australia has also negotiated with the EU on PNR and has instituted an Electronic Travel Authority (ETA). Australia and New Zealand lead efforts within the region and throughout the international community to promote the APEC Privacy Framework.

16.2.3. The Americas

The Department has several information sharing programs that involve the cooperation of Latin American countries. To support these efforts, the DHS Privacy Office worked to increase its understanding of privacy policies and legislation in the region. The DHS Privacy Office established contacts with several Latin American countries through its participation in the IberoAmerican Data Protection Network (RIPD) meeting, held May 27-29, 2008, in Cartagena, Colombia. The gathering, organized by the Spanish Data Protection Authority, included sixteen (16) Latin American countries, as well as representatives from the EU Commission and the Portuguese Data Protection Authority. The Chief Privacy Officer presented an overview of the U.S. privacy framework, stressing the compatibility and necessity of security and privacy protections. He elaborated on the tools DHS uses to ensure the FIPPs are implemented throughout Departmental programs and policies. We expect the Office will continue to build its relationships with Latin America during the next reporting year.

As the Department increases its contacts with friends and allies abroad, the Privacy Office is inviting counterparts in other governments to participate in staff exchanges. The goal of these exchanges is to share best practices and to promote understanding of one another's systems of protecting personal information held by the government. The Privacy Office was pleased to host its first exchange with Canada from September 10 to 21, 2007. Given our shared border and ideals regarding security and privacy, Canada is an important international partner for the Office. Because Canada is a member of the OECD, APEC, and the International Conference of Data Protection and Privacy Commissioners, its privacy officials offer a unique perspective on global privacy issues. Two audit specialists from the Office of the Privacy Commissioner of Canada, Mike Fagan and Tom Fitzpatrick, attended meetings and briefings to understand the privacy compliance process and how the Privacy Office works collaboratively with our programs to incorporate privacy into the design phase. Mr. Fagan and Mr. Fitzpatrick also provided in depth briefings on the Canadian Privacy Commissioner's office and the role of Privacy Impact Assessments in assuring compliance. While in Washington Mr. Fitzpatrick and Mr. Fagan were able to attend a Data Privacy Integrity Advisory Committee (DPIAC) meeting, tour the White House, Capitol Hill, and also meet with Congressional Government Accountability Office (GAO) representatives to acquire a better understanding of our compliance program.

In February 2008, the Chief Privacy Officer was the keynote speaker at the 9th Annual Privacy and Security Conference convened by Reboot Communications Limited in Victoria, Canada. In his keynote address to more than 900 attendees, he spoke about privacy issues DHS faces daily, pointing out the particular challenge of protecting privacy while sharing personal information with U.S. allies as needed. The Chief Privacy Officer emphasized the Department's efforts to protect the privacy of U.S. citizens and citizens of other countries who visit the U.S.

Throughout the reporting period, the Privacy Office has coordinated with the Canadian Privacy Commissioner's Office, as well as the provincial offices of Ontario and British Colombia. Ken Anderson, Assistant Privacy Commissioner for Ontario, presented on Ontario's policy toward CCTV cameras in public spaces at the DHS Privacy Office's conference on CCTV cameras.

16.2.4. Israel

In April, the Office was pleased to host Yoram Hacohen, Head of the Israeli Law, Information and Technology Authority and the Databases Registrar (ILITA). The Israeli Ministry of Justice established ILITA in 2007 to strengthen the protection of privacy in Israel. During his visit, Mr. Hacohen and Privacy Office staff discussed the effectiveness of considering privacy requirements at the design phase of policies and programs. As part of his visit, the Office coordinated a tour and briefing with the Department's US-VISIT program. ILITA is a December 2007 recipient of the European Commission's Twining Program on data protection, which aims to ensure the effective enforcement of national legislation on privacy in line with European standards and to raise public awareness of personal data protection.

16.3. Multilateral Representation

Through participation in multilateral organizations, the DHS Privacy Office continues to broaden its global perspective and engage in a range of privacy-related issues. To build trust with international partners and the traveling public, the Office engages in speaking events and publishes articles in widely-circulated privacy periodicals. Specific Office activities are discussed in the following subsections.

16.3.1. Organization for Economic Cooperation and Development

The DHS Privacy Office continued to contribute to the Organization for Economic Cooperation and Development's (OECD) work on enforcement of cross-border privacy rules and monitored its application to civil and regulatory enforcement. The DHS Privacy Office participated in the OECD's Working Party on Information and Privacy (WPISP) meetings in Ottawa, Canada and Paris, France. Throughout the reporting period, the DHS Privacy Office created, reviewed, and contributed to U.S. interagency position papers for various OECD agenda items. Of particular interest is a proposal initiated by the Secretariat for a "global privacy dialogue" that is intended to revisit the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Through this initiative, the DHS Privacy Office plans to engage WPISP members in a discussion of best practices at upcoming meetings scheduled during next year's reporting period.

16.3.2. International Conference of Data Protection and Privacy Commissioners

In September, the Office continued its participation as an official observer to the International Conference of Data Protection and Privacy Commissioners in Montreal, Canada. This is the largest annual meeting of data privacy authorities and a significant opportunity to discuss privacy developments world-wide. Based on its positive relationship with the Canadian Privacy Commissioner, the host for the 2007 conference, the Office was able to provide Secretary Chertoff an opportunity to deliver the opening-day keynote address. His address sent the strong message to participants from 78 countries that the Department is committed to privacy. The DHS Privacy Office's Director of Compliance also spoke on a panel and highlighted the Department's practical application of the FIPPs to Department programs through PIAs. The DHS Privacy Office, together with representation from the Federal Trade Commission, the Department of Justice, the Department of Commerce, the Social Services Administration, and the Department of Health and Human Services, formed the U.S. delegation for this event. Significantly, this year's Commissioners' resolution included formal recognition that countries have adopted different approaches to protecting personal information and enhancing privacy rights.

16.3.3. International Working Group on Data Protection in Telecommunications (Berlin Group)

The DHS Privacy Office attends the biannual Berlin Group meetings as an observer. The Berlin Group, organized by the Data Protection Authority of Berlin, Germany, focuses on privacy issues related to IT and telecommunications in both the commercial and government contexts. These meetings are an excellent opportunity to hear data protection officials discuss current topics and to exchange ideas on improving privacy in telecommunications and media.

During this reporting period, the DHS Privacy Office attended the September 4-7, 2007, meeting in Berlin, Germany, where the Group reviewed EU Member State authorities' policies on data mining and the collection and use of PII to capture tax evaders. The DHS Privacy Office also attended the March 3-4, 2008, meeting in Rome. Among the topics at this meeting were use of spyware for law enforcement purposes and a formal recommendation on the implementation and application of the Council of Europe Convention No. 185 on Cybercrime, a major international co-operation tool with a view to harmonizing criminal offences, investigation procedures, and judicial and police assistance. The next meeting, to be held in October on the margins of the 30th annual International Conference of Data Protection and Privacy Commissioners, will include discussions on biometric encryption, storage of SMS messages for law enforcement purposes, and international standards in privacy.

16.3.4. International Organization for Standardization

The International Organization for Standards (ISO) is an internationally recognized standards development body. The ISO's Subcommittee 27/Working Group 5 is in the process of developing non-technical privacy standards. These standards, labeled ISO 29100 – A Privacy Framework, will be "a framework for defining privacy safeguarding requirements as they relate to PII processed by any information and communication system in any jurisdiction," and may affect the privacy policy and legislation of many DHS partners. During this report period, the DHS Privacy Office reviewed drafts of the working documents and shared its views with the U.S. representatives to SC27/WG5. The DHS Privacy Office will continue to monitor developments of this ISO proposal.

16.3.5. Academy of European Law Conference

As part of the Office's continued development of international privacy expertise, the Associate Director for International Privacy Policy attended the Academy of European Law (ERA) Conference in Trier, Germany, titled "Data Exchange and Data Protection in the Area of Freedom, Security, and Justice." ERA is a public foundation that works to foster a better understanding of EU laws through various activities, including conferences. The Conference offers a first-hand opportunity to learn from representatives of EU security and law enforcement institutions as well as the European Data Protection Supervisor and academic privacy advocates. Understanding this topic is essential to DHS discussions regarding information sharing with EU and Member State partners and has provided useful insights for U.S. Government positions.

16.3.6. International Chamber of Commerce Conference

The International Chamber of Commerce (ICC) is an organization focused on fostering global commerce, including standards development. The Associate Director for IPP attended the May 28, 2008, ICC Conference, "A Global Perspective on Data Protection and Processing," in Paris, France. Conference attendees from the private sector voiced concern over the diverse and often conflicting EU Member State standards for personal information exchange in the commercial context, and the unsuitability of mechanisms for compliance. Discussion took place against the backdrop of presentations on the developments in the APEC region and the recommendation in the 1980 OECD Privacy Guidelines that members avoid creation of obstacles to data flows in the name of privacy protection. This discussion is significant because the EU Data Protection Directive is a potential model for future EU regulation of data flows in the law enforcement and security context. Understanding the discussions around global regulation of data flows aids the Department in addressing potential concerns over cross border activities and promotes the U.S. privacy framework as an effective means to protect personal information.

16.3.7. Speaking to U.S.-Based Audiences

The Department relies on the cooperation and support of the U.S. private sector in pursuing its mission. The DHS Privacy Office reaches out to American privacy professionals to increase knowledge and appreciation of how the Department implements privacy protections in its programs and our position on international privacy matters. Highlights of U.S.-based activities include the following:

- October 2007: The Deputy Chief Privacy Officer moderated a panel at the International Association of Privacy Professionals' annual Privacy Academy in San Francisco, California, titled "Government to Government Cross Border Sharing of Privacy Information for Law Enforcement & Homeland Security Purposes." Panel members included the Data Protection Commissioners of Ireland and Canada.
- January 2008: The Deputy Chief Privacy Officer participated in a panel titled "Privacy and National Security," at the Duke University School of Law conference commemorating the EU's Data Protection Day.
- May 2008: The Chief Privacy Officer addressed the Association of Corporate Travel Executives at the annual meeting by participating in a panel titled "Global Data Protection and Security Issues: How Safe We Are in 2008," and fielded questions on border searches, PNR data sharing, and the privacy rights of non-U.S. persons.
- June 2008: The Chief Privacy Officer spoke to the German-American Lawyers' Association regarding the role of the DHS Privacy Office in U.S. Government collection and use of personal information for the maintenance of secure and open borders.

16.3.8. Publications

Contributing articles in respected publications is another means for the DHS Privacy Office to communicate with the public and shape policy. The DHS Privacy Office published the following articles on international privacy policy issues during this reporting period:

- "A way ahead for global privacy standards? Thoughts on a UN Convention on Data Protection, International Standards and International Agreements. Which is the Best Option?" Privacy Laws & Business, Issue 89, October 2007. This article discussed the outlook for global privacy standards, emphasizing that broad adoption of any standard by the public and private sectors will have to reflect the values of those nations that handle a substantial amount of personal information.
- "DHS defends PNR programme against 'misplaced' EU criticisms", Data Protection Law & Policy, Volume 04 Issue 11, November 2007. This article discussed DHS privacy practices in response to misplaced criticism in the European press and from European Data Protection Authorities.
- Short articles published throughout the reporting period in the International Association of Privacy Professionals' The Privacy Advisor regarding the exchange of data between EU Member States on short stay-visas, the proposed ISO Privacy Framework, the EU Parliament opinion on the U.S. – EU PNR agreement, German spyware and surveillance, and the IberoAmerican Data Protection Network meeting.

17. Reports

17.1. Section 803 Reports

Section 803 of the 9/11 Commission Act established additional privacy and civil liberties requirements for DHS. For the purposes of Section 803 Reporting, DHS currently reviews the following activities:

- Privacy Threshold Analyses;
- Privacy Impact Assessments;
- System of Records Notices and associated Privacy Act Exemptions;
- Privacy Act (e)(3) Statements;
- Computer Matching Agreements; and

- Privacy protection reviews of Information Technology and Program Budget requests, including OMB 300s (discussed in Section 2.5 of this report) and Enterprise Architecture Alignment Requests through DHS's Enterprise Architecture Board.[63]

The following sections contain the information reported by DHS during the current DHS Privacy Office Annual Report to Congress reporting period for each activity listed above.

17.1.1. Reviews

The table below shows the types and number of reviews conducted by DHS during this reporting period.

Type of Review	Number of Reviews
Privacy Threshold Analyses	170
Privacy Impact Assessments	27
System of Records Notices and associated Privacy Act Exemptions	10
Privacy Act (e)(3) Statements	3
Computer Matching Agreements	0
Data Mining Reports	1
Privacy Protection Reviews of IT and Program Budget requests	14
Total Reviews for FY08	*225*

17.1.2. Advice and Responses

For purposes of Section 803 reporting, advice and response to advise includes the issuance of written policies, procedures, guidance, or interpretations of privacy requirements for circumstances or businesses processes written by the Privacy Office and approved by DHS leadership. During the reporting period, DHS released the following guidance related to privacy:

- Sensitive System Handbook 4300 and 4300A, updated to include additional, privacy-related requirements.

[63] The Enterprise Architecture Board operates through the OCIO and performs substantive and strategic reviews of all requests for new IT initiatives through its operational sub-organization, the Enterprise Architecture Center of Excellence (EACOE). The Privacy Office sits on the EACOE and reviews each request for new technology to ensure that all DHS use of technology sustain privacy protections.

- Appendix S of 4300A: Compliance Framework NIST SP 800-53 Controls for Privacy Sensitive Systems.
- Official DHS System of Records Notice (SORN) Guidance, providing guidance on how to write a SORN.
- Updated Privacy Threshold Analysis.
- Privacy Act Statement Guidance as related to (e)(3) of the Privacy Act.

Each of these documents is described further in Section 2 of this report.

During the reporting period, DHS conducted the following training:

- DHS personnel and contractors took classroom-based privacy training courses in 3,795 instances.
- DHS personnel and contractors took computer-assisted privacy training courses in 61,675 instances.[64]
- DHS Privacy Office provided ten in-person privacy training courses to DHS personnel and contractors.

Additional component activities are described in section 3 of this report.

Section 803 Reports also include the number of complaints the DHS Privacy Office and components received during the reporting period. Descriptions of these complaints, as well as the reported metrics, are provided in Section 9 of this report.

17.2. Section 804 Data Mining Reports

The DHS Privacy Office has submitted three reports to Congress on the Department's data mining activities since 2006. On July 6, 2007, the Office issued the second of these reports, entitled *2007 Data Mining Report: DHS Privacy Office Response to House Report 109-699* ("2007 Data Mining Report"). The 2007 Data Mining Report described Department activities that fit the definition of "data mining" set forth in House Report No. 109-699 – *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes*[65] and discussed progress to date on the recommendations for protecting privacy in Department data mining activities set out in the DHS Privacy Office's 2006

[64] DHS offers multiple computer training courses. An individual may have taken multiple courses if their current job requires such training. This number includes annual privacy awareness training for the USCG and ICE.

[65] Conference Report on HR 5441, DHS Appropriations Act, House Rept. No. 109-699, Sept. 28, 2006, H7784, at H7815.

Report.[66] The DHS Privacy Office also stated that it was considering holding a public workshop to explore appropriate privacy protections, including the use of anonymization tools.[67]

After the DHS Privacy Office issued the 2007 Data Mining Report, the 9/11 Commission Act was enacted.[68] In response to the *Federal Agency Data Mining Reporting Act of 2007*, the DHS Privacy Office issued its *Letter Report Pursuant to Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007* ("Letter Report"), on February 11, 2008, which provided a preliminary analysis of relevant DHS data mining activities, with the understanding that a comprehensive report would follow. The Letter Report reiterated the Office's interest in holding a public workshop to discuss the privacy impacts of government data mining, to identify ways of validating data mining models, and to highlight technology tools that could both enhance privacy and support data mining research.[69] A copy of the Letter Report is available on the DHS Privacy Office website.[70]

The DHS Privacy Office held the public workshop, *Implementing Privacy Protections in Government Data Mining,* on July 24-25, 2008, to inform its 2008 report to Congress on Department data mining activities.[71] This workshop is discussed in Section 12.3.3 of this report. A summary of lessons learned at the workshop will be included in the Office's 2008 report to Congress.

18. Departmental Disclosure and Freedom of Information Act Program

FOIA is a pillar of the U.S. privacy protection framework. In accordance with Executive Order 13392, *Improving Agency Disclosure of Information*, signed by President Bush on December 14, 2005, DHS Secretary Chertoff designated the Chief Privacy Officer as the DHS Chief FOIA Officer. The Chief Privacy Officer'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, the Chief Privacy Officer appointed two positions, a Deputy Chief FOIA Officer and a Director of Departmental Disclosure and FOIA. The DHS Disclosure and FOIA group also has four full-

[66] 2007 Data Mining Report at 33-36. The 2006 report, entitled *Data Mining Report: DHS Privacy Office Response to House Report 108-774,* was issued on July 6, 2006. All Privacy Office reports are available on the DHS Privacy Office website at www.dhs.gov/privacy.

[67] 2007 Data Mining Report at 34.

[68] Public Law No. 110-53, 121 Stat. 266.

[69] Letter Report at 4.

[70] www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2008.pdf

[71] The Federal Register Notice announcing the workshop, the workshop agenda [and transcript], and public comments submitted in response to the Notice, are all available on the Office's website at www.dhs.gov/privacy.

time employees in the positions of Associate Director of Operations, Associate Director of Policy and Program Development, and two FOIA Program Specialists, along with three full-time contractors that specifically support the Disclosure and FOIA group.

The sections below highlight several key FOIA activities. Additional information will be available in the FY08 Annual FOIA Report, scheduled to be published in spring 2009.

18.1. Compliance with Executive Order 13392

In response to the deliverables required by the Executive Order 13392, the Disclosure and FOIA group drafted two DHS improvement plans. The first FOIA Improvement Plan, released in summer 2006, provided a general overview of DHS FOIA operations. The revised FOIA Improvement Plan, issued in January 2007, included concrete milestones, specific timetables, achievable outcomes, and metrics to measure success, while also focusing on particular components with large backlogs.[72] Of the 39 milestones listed in the 2007 Annual FOIA Report to DOJ, DHS has fully met 29. For the 10 milestones not yet met, the Disclosure and FOIA group is working to address the unique circumstances at individual components and reach the remaining milestones. In furtherance of the Executive Order mandate to make FOIA programs more citizen-centered, the Disclosure and FOIA group continues to assess the staffing, technological, and educational needs of every DHS FOIA program.

As part of the June 1, 2007, report to the President on agency progress under Executive Order 13392, the Attorney General required agencies with FOIA requests or administrative appeals pending beyond the statutory time period (i.e., a backlog) at the end of Fiscal Year 2007, to establish backlog reduction goals for the next three fiscal years. DHS posted these goals on the agency's FOIA web site by November 1, 2007, as required. All components are currently working toward their backlog elimination goals as set for FY08. The Disclosure and FOIA group notifies each component regarding their progress against their target completion rates every month.

Another milestone in the FOIA Improvement Plan was completing the final FOIA regulations. In January of 2008, the Disclosure and FOIA group drafted the Department's final FOIA regulations, which are currently under internal review. The target date for the regulations to go into effect is December 31, 2008.

While much progress was made over the past year, one area in which the Department's FOIA program needs improvement lies within this area. FEMA and CBP, for example, were the only DHS components that failed to meet their hiring goals or fully implement planned operational improvements outlined in the DHS Revised FOIA Improvement Plan. In addition, FEMA failed to meet its published goal of ensuring that FOIA professionals attend DOJ or

[72] The *DHS FOIA Revised Operational Improvement Plan* can be found at http://www.dhs.gov/xlibrary/assets/foia/privacy_foia_improvement-plan_r.pdf.

commercial FOIA training. These shortcomings, coupled with continued customer service gaps that exist, particularly at the aforementioned components as well as the USCG and TSA, lead the Chief FOIA Officer to call for better efforts to ensure these programs remain citizen-centered and results-oriented. Better efforts to reduce the existing FOIA backlogs, as well as the volume of service-related complaints, particularly at these components, are necessary to ensure complete compliance with Executive Order 13392.

18.2. Implementation of the OPEN Government Act of 2007

The *Openness Promotes Efficiency in our National (OPEN) Government Act of 2007*("OPEN Government Act"), signed by President Bush on December 31, 2007, amends FOIA and codifies many of the provisions in Executive Order 13392. The OPEN Government Act established a definition of news media representatives, to ensure that the FOIA Offices consider the continuing evolution of methods of news delivery, such as freelance journalists, that distribute a "distinct work" to a public audience. The OPEN Government Act also directed that court awarded attorneys' fees be paid from an agency's own appropriation, prohibits agencies from assessing certain fees if it fails to comply with FOIA deadlines, and established an Office of Government Information Services at NARA to review agency compliance with FOIA. On February 5, 2008, the Disclosure and FOIA group issued Department-wide guidance regarding the implementation of the OPEN Government Act, highlighting both ways in which the Department was already compliant with the Act and improvements necessary for statutory compliance.

The OPEN Government Act included new reporting requirements for the FY08 Annual FOIA Report to DOJ. Most notably, all components are required to report the following:

- Number of times the component relied upon each b(3) (statutory specific) exception;
- Average and median initial request and appeal response times;
- Request counts by response times (i.e. number of requests responded to within 0-20 days, 21-40 days, in 20-day increments up to 300 days and between 301-400 days);
- List of the agency's ten oldest pending requests and appeals;
- Accounting of requests seeking expedited treatment;
- Accounting of all fee waiver assessment requests; and
- More detailed reporting of consultations received from other agencies.

In an effort to ensure timely compliance, the Disclosure and FOIA group prepared briefings and outlines for each component to inform them of the new reporting requirements for the FY08 Annual FOIA Report to DOJ under the OPEN Government Act. Agencies are required to report data for each component and for the agency as a whole. The Disclosure and FOIA

group compiles all data submitted by the components and prepares the overall report for the agency.

18.3. 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. USCIS, which receives the greatest volume of FOIA requests in DHS, recently finalized a contract to bring in more FOIA personnel. Additionally, USCIS implemented an online tool through which customers may access information pertaining to their current status in the request backlog queue in relation to the total number of pending requests. Lastly, effective August 2008, USCIS will remove certain requests from the FOIA processing queues and more appropriately process them under a fee-for-service arrangement.

During the reporting period, the Department's FOIA leadership continued working to merge the processes of multiple component agencies into a single program to support DHS as a whole. Most components actively participated in Department-wide FOIA initiatives to enhance responsibility and accountability, manage workload, and implement guidance provided by the Disclosure and FOIA group. The Disclosure and FOIA group provided direction regarding which DHS components have responsibility in cases where files are shared between components and coordinated Department-wide responses. The DHS FOIA leadership also issued Department-wide guidance on the management of FOIA requests seeking agency records regarding ongoing law enforcement investigations and the treatment of DHS personnel information contained within agency records processed pursuant to the FOIA, in an effort to ensure consistent responses to FOIA requests throughout the Department.

Unlike the Privacy unit, the FOIA unit experiences uneven and limited cooperation and coordination between the Chief FOIA Officer and the component FOIA Officers. Nevertheless, generally speaking, DHS components complied with the Department-wide guidance. One notable exception is the USCG, which has refused to comply with the Chief FOIA Officer's guidance on requests seeking agency records regarding ongoing law enforcement investigations. The Chief FOIA Officer's guidance mirrors guidance on the matter from the U.S. Department of Justice, Office of Information and Privacy (OIP).

In addition to policy and program development activities, the Disclosure and FOIA group continues to process FOIA requests for the DHS Headquarters programs, including the Office of the Secretary. Additionally, the Director, Disclosure & FOIA served as a liaison to DHS Directorates and components, forwarding FOIA and Privacy Act requests seeking records they maintain. The Disclosure and FOIA Group was instrumental in standing up FOIA offices and appointing FOIA Officers for four DHS Headquarters components in 2007. CRCL, Office of

Management (MGMT), Office of Policy, and Office of the General Counsel (OGC), now receive and process their own FOIA requests. The Associate Director of Policy and Program Development provides basic FOIA and PA training to all new DHS employees and offers FOIA and PA training to all DHS components on an as-needed basis to cultivate FOIA knowledge and expertise agency-wide.

The Deputy Chief FOIA Officer represents the Department at quarterly meetings of the DOJ's OIP FOIA Officer's 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 may affect the government's ability to invoke FOIA exemptions to protect sensitive homeland security information, as well as procedural matters relating to homeland security.

The Disclosure and FOIA group 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 disclosure within the Department. Additionally, the Deputy Chief FOIA Officer speaks and participates in many DHS component events to foster Department-wide knowledge regarding responsibilities and compliance under the Statute.

One limitation faced by the Chief FOIA Officer is the lack of authority over the component FOIA Officers as the component programs are decentralized. The DHS Chief FOIA Officer must rely upon the components to hire qualified FOIA Officers to effectively manage the component's FOIA program and implement Departmental guidance.

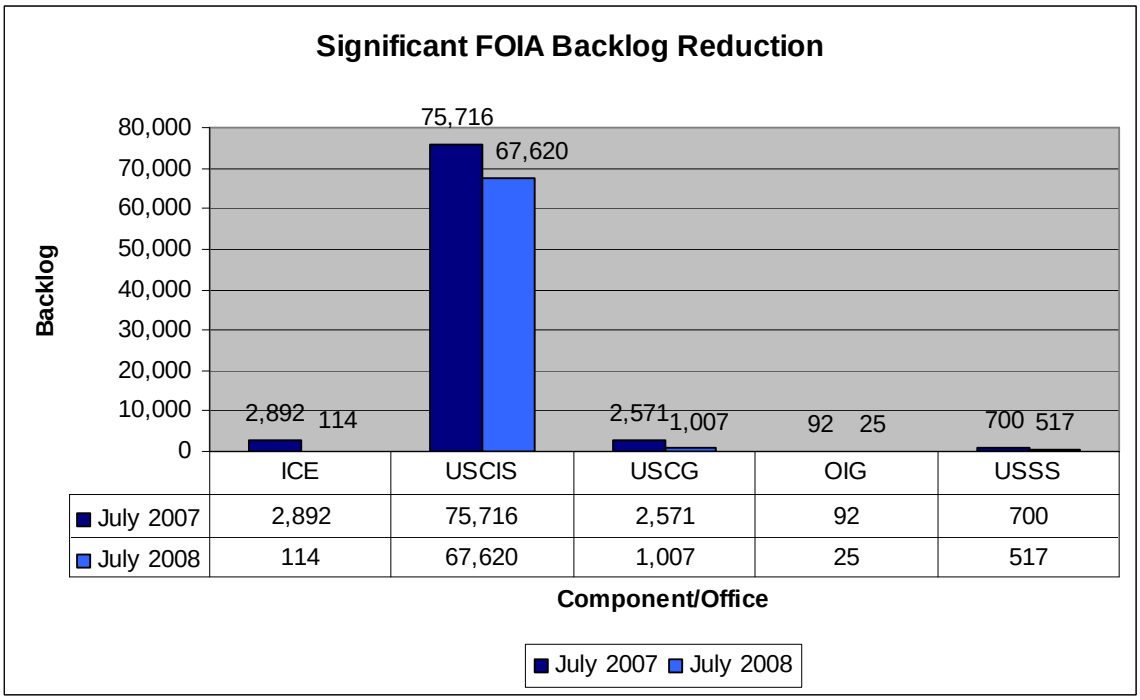
18.4. Annual FOIA Report to DOJ

DHS programs and policies continue to be the subject of numerous FOIA requests because of high public interest in its operations. The Department's FOIA Program is centralized for purposes of establishing policy, and managerially and operationally decentralized in each component. As reported in the FY07 DHS Annual FOIA Report, the combined centralized and decentralized elements of the program cost an estimated $25 million to run annually. FY07 incoming requests numbered 108,416, while the Department processed 135,297 incoming requests and granted 76,440 requests in full or in part. The DHS Disclosure and FOIA group received 1,118 initial requests in FY07. By mid-way though FY08, the group received 692, including 124 complex cases requiring searches and coordination with multiple DHS components. The FY08 Annual FOIA Report is scheduled to be published in spring 2009.

18.5. 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. The Chief FOIA Officer and Deputy Chief FOIA Officer are working with component leadership to devote adequate resources to their FOIA programs. Recently, the

GAO noted in its report, "*Freedom of Information Act-Agencies Are Making Progress in Reducing Backlog, but Additional Guidance is Needed*," (March 14, 2008) that notably DHS decreased its backlog of overdue requests by 29,972, or about 29%. The Attorney General's report to the President pursuant to Executive Order 13392, "*Improving Agency Disclosure of Information*," released May 30, 2008, lauded the Department's reduction of the number of pending requests by 26,881 in FY07 and the additional 23,354 requests processed beyond the number processed in FY06. The following graph depicts components that made significant progress in reducing their backlog from July 2007 to July 2008. Together, these groups represent 15% of the 29% reduction noted above.



18.6. FOIA Staffing

The seven operational components have varying levels of staffing and leadership. The below chart identifies the pay-grade of component FOIA leadership, which may serve as a reflection of experience-level and the importance placed on FOIA, in each of the seven operational components.

This chart also indicates the number of personnel currently processing[73] FOIA requests within the seven operational components.

Component	Grade-level of FOIA Officer	Number of Processors Full/Part-Time
CBP	GS 15	10/53
CIS	SES	58/0
FEMA	GS 14	4/10
ICE	GS 15	25/53
TSA	GS 15	11/0
USCG	GS 14	17/430
USSS	GS 15	11/32

[73] This number includes personnel that are FOIA Points of Contact in the field offices as a collateral duty. These personnel are responsible for coordinating the search for records and preparing withholding justifications.

19. Appendix A: Published Privacy Impact Assessments

The table below lists all published PIAs from July 1, 2007, through July 1, 2008.

Component	Name of System	Date Approved
CBP	Secure Border Initiative-net (SBInet)	7/20/2007
US-VISIT	US- VISIT Arrival and Departure Information System-long	8/1/2007
CBP	Automated Targeting System - update	8/3/2007
CBP	Advance Passenger Information System 2007	8/8/2007
TSA	Secure Flight- 2007	8/9/2007
CBP	Western Hemisphere Travel Initiative-Land and Sea Rule	8/9/2007
CIS	Verification Information System Update	9/6/2007
CBP	APIS Update - General Aviation	9/12/2007
MANAGEMENT	Personnel Security Activities Management System	9/12/2007
TSA	Large Aircraft Security Program	9/21/2007
TSA	Transportation Worker Identification Credential Program - Update	10/4/2007
TSA	Universal Commercial Driver's License Security Threat Assessment	10/15/2007
TSA	Visitors Management System Update	10/22/2007
TSA	Airman Certificate Vetting Program	10/22/2007
US-VISIT	United States Visitor and Immigrant Status Indicator Technology Program- 10 Print update	11/16/2007
CIS	DHS UKVisa Program	11/16/2007
NPPD	National Infrastructure Coordination Center INSight Application	11/29/2007
MANAGEMENT	Executive Correspondence Tracking	11/29/2007
DHS Wide	DHSAccessGate	11/29/2007
TSA	Boarding Pass Scanning System	11/30/2007
DHS Wide	REAL ID Final Rule	1/6/2008
TSA	Whole Body Imaging	1/13/2008
ICE	ICE Pattern Analysis and Information Collection	1/22/2008
TSA	Federal Flight Deck Officer Program	1/22/2008
OIG	OIG Investigative Data Management System	1/22/2008
MANAGEMENT	Personnel Security Activities Management System Update	1/22/2008
CBP	Western Hemisphere Travel Initiative-Technology	1/23/2008
TSA	Crew Member Self Defense Training	2/6/2008
CIS	Verification Information System update	2/22/2008
CIS	United States Citizenship and Immigration Services Person Centric Query Service Update Verification Information System	2/22/2008
CIS	United States Citizenship and Immigration Services Person Centric Query Service Update National Security and Records Verification Directorate/Verification Division	2/22/2008
S & T	Project Hostile Intent	2/25/2008
S &T	PREDICT	2/27/2008
DHS Wide	e-Recruitment	3/4/2008

Component	Name of System	Date Approved
USCG	Biometrics at Sea	3/14/2008
CBP	WHTI Land and Sea FR	3/25/2008
USCG	Law Enforcement Intelligence Database	4/2/2008
USCG	Maritime Awareness Global Network	4/14/2008
US-VISIT	US-VISIT Exit	4/15/2008
S & T	Group Violent Intent Modeling Project	4/25/2008
MANAGEMENT	Web Time and Attendance System	5/2/2008
NPPD	Einstein 2	5/19/2008
TSA	Tactical Information Sharing System	6/2/2008
CBP	Electronic Travel Authorization	6/2/2008
TSA	Security Threat Assessment for Airport Badge and Credential Holders	6/2/2008
US-VISIT	Technical Reconciliation and Analysis Classification System	6/06/08
S & T	Critical Infrastructure Change Detection	6/25/2008
US-VISIT	United States Visitor and Immigrant Status Indicator Technology Program/Department of Homeland Security and the United Kingdom Border Agency's International Group Visa Services Project	7/1/2008

20. Appendix B: Systems of Records Notices

The table below lists all SORNs completed by DHS from July 1, 2007, through July 1, 2008.

Component	Name of System	Date Published in Federal Register
CBP	**DHS/CBP-006** Automated Targeting System (71 FR 64543)	8/6/2007
US-VISIT	**DHS/USVISIT-001,** Arrival and Departure Information System (ADIS) 12/12/2003 68 FR 69412	8/22/2007
TSA	**DHS/TSA 019**, Secure Flight Records	8/23/2007
CBP	**DHS/CBP-005**, Advanced Passenger Information (APIS)	8/23/2007
TSA	**DHS/TSA 019**, Secure Flight Records	11/9/2007
ICE	**DHS/ICE-002,** ICE Pattern Analysis and Information Collection (ICEPIC)	1/30/2008
USCIS	**DHS/USCIS-004** Verification Information System	2/28/2008
DHS	**DHS/ALL-004,** General Information Technology Access Account Records System Update	5/15/2008
USCG	**DHS/USCG-061,** Maritime Awareness Global Network	5/15/2008
USCG	**DHS/USCG-062,** Law Enforcement Intelligence Database	5/15/2008
IA	**DHS/IA-001,** Enterprise Records System	5/15/2008
CBP	**DHS/CBP-009,** Electronic System for Travel Authorization (ESTA)	6/10/2008
US-VISIT	**DHS/NPPD/USVISIT-003,** Technical Reconciliation Analysis Classification System (TRACS)	6/16/2008