DHS Privacy Office

Annual Report to Congress

July 2008 – June 2009

September 2009

Homeland Security

Message from the Chief Privacy Officer

The DHS Privacy Office is proud to present its fifth Annual Report covering the time period from July 2008 through June 2009. This report, as well as previous reports, can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

The change of presidential administrations during this reporting period also represented a time of transition for the DHS Privacy Office. I began my tenure as the Chief Privacy Officer in March, and immediately began to build upon and strengthen the legacy of diligence and dedication found in the DHS Privacy Office and throughout the Department. I hope to combine the breadth of my prior experience with the institutional knowledge of the DHS Privacy Office in order to advance a culture of privacy throughout the Department.

I share the Administration's vision to ensure the public trust and establish a system of transparency, public participation, and collaboration. In this new era of openness in government, we at the DHS Privacy Office strive to be true stewards of the citizens we serve. It is, therefore, my goal to see privacy considerations addressed systematically throughout the Department. To that end, we are engaged with Department leadership in establishing privacy officers within each of the operational components that do not as yet have such resources. Privacy officers in each component will help ensure privacy protections are implemented in the planning and development of each program, technology and/or policy within the Department. In addition, we are participating in numerous departmental working groups and attend the daily and weekly departmental leadership meetings to provide privacy expertise at the highest levels within the Department. Finally, we are actively engaging in outreach to promote privacy awareness, both throughout the federal government and to the public.

We stand at a crossroads – where we have great opportunities to advance privacy and transparency on multiple fronts. The DHS Privacy Office has already begun implementation of a two-pronged outreach strategy focused on privacy education. This approach allows the DHS Privacy Office to provide deliberate and specific messaging and outreach inside DHS and the government, as well as to the public. As a support component, the inward facing prong of the DHS Privacy Office's strategy includes an ongoing education program to create a culture of privacy awareness and compliance throughout the Department. This part of the outreach program also encompasses full compliance with the Freedom of Information Act (FOIA) to ensure that our mission and statutory requirements are met. The external approach provides continuing education to reaffirm to the public, both nationally and internationally, the Department's commitment to respecting the privacy rights of all people, and the Department's commitment to quick resolution of FOIA and redress requests.

The DHS Privacy Office continues to be at the forefront of privacy issues affecting the Department and the federal government. I am excited by this new era and look forward to advancing the DHS Privacy Office into an even more productive future.

Mary Ellen Callahan
Chief Privacy and Freedom of Information Act Officer
United States Department of Homeland Security

Executive Summary

The Department of Homeland Security Privacy Office (DHS Privacy Office or Office) is the first statutorily created privacy office in any federal agency, as set forth in 6 U.S.C. § 142, § 222 of the Homeland Security Act, as amended. The mission of the DHS Privacy Office is to preserve and enhance privacy protections for all individuals, to promote transparency of DHS operations, and to serve as a leader in the federal privacy community. The Office accomplishes its mission by focusing on three key activities: (1) requiring compliance with the letter and spirit of federal laws promoting privacy and centralizing Freedom of Information Act (FOIA) and Privacy Act operations within the DHS Privacy Office to provide policy and programmatic oversight and support operational implementation within the components; (2) providing education and outreach to build a culture of privacy and adherence to Fair Information Practice Principles (FIPPs) across the Department; and (3) communicating with the public through published materials, formal notice, public workshops, and meetings.

This report will provide a more detailed explanation of the activities of the DHS Privacy Office, and the various methods employed in order to ensure that privacy is given appropriate consideration, weight, and protection throughout the Department. The DHS Privacy Office works as a whole to advance privacy throughout the Department, but is divided into two major functional units: Privacy Compliance; and Departmental Disclosure and FOIA. The DHS Privacy Compliance Group (Compliance Group) manages statutory and policy-based responsibilities by working with each component and program throughout the Department to ensure that privacy considerations are addressed when implementing a program, technology, or policy. The Departmental Disclosure and FOIA Group (Disclosure and FOIA Group) works with each component to ensure consistent compliance with the FOIA throughout the Department.

While Compliance and FOIA form the largest structural units in the DHS Privacy Office, the Office also places great emphasis on cross-cutting, topics salient to both privacy and homeland security that support compliance and disclosure. For example, as described in this report, many aspects of the work undertaken by the DHS Privacy Office encompass some form of education, whether internal to the Department or external to the public. The DHS Privacy Office conducts internal education and training; furthermore, its policy initiatives are meant to educate and inform departmental activities such as information sharing. DHS Privacy Office's engagement with the public promotes awareness and understanding of issues such as redress opportunities and transparency.

The DHS Privacy Office also strives to be a leader at the forefront of emerging privacy issues. The dynamic nature of privacy issues related to homeland security requires that the DHS Privacy Office be especially agile in protecting privacy as it relates to topics such as information sharing, fusion centers, cybersecurity, and social media. This report details the DHS Privacy Office activities and initiatives during this reporting period in each of these areas.

Figure 1 on the following page depicts the implementation elements that comprise the "Culture of Privacy" at DHS. Each of its eleven elements make an important contribution to the development of a privacy culture; and the specific privacy activities described in this Annual Report often touch on more than one of these elements. The Culture of Privacy graphic appears to the right of each section of the Annual Report to indicate which implementation element(s) the section addresses. The Chief Privacy Officer along with the DHS Privacy Office uses these elements to build a strong privacy program at the Department – one that is recognized as among the leading privacy offices in the federal government.

Figure 1: Culture of Privacy Implementation Elements

Table of Contents

List of Figures

List of Tables

I. Background

A. About the Office

The DHS Privacy Office is the first statutorily mandated privacy office in the federal government. Its mission is to minimize the impact on an individual's privacy, particularly an individual's personal information and dignity, while achieving the Department's mandate. The Chief Privacy Officer reports directly to the Secretary of the Department, and the Office's mission and authority are founded upon the responsibilities set forth in section 222 of the Homeland Security Act of 2002, as amended.[1] With the change of presidential administrations during this reporting period, the DHS Privacy Office operated under the leadership of Hugo Teufel III, Chief Privacy Officer (July 1, 2008 to January 20, 2009); John Kropf, Acting Chief Privacy Officer (January 20, 2009 to March 9, 2009); and Mary Ellen Callahan, Chief Privacy Officer (March 9, 2009 to present).

Not only does the DHS Privacy Office serve as the steward of section 222 of the Homeland Security Act, it also ensures that the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act of 2002, and the numerous laws, Executive Orders, court decisions and Departmental policies that protect the collection, use, and disclosure of personal and Departmental information are all followed. The Privacy Act of 1974 embodies a code of fair information principles that govern the collection, maintenance, use, and dissemination of personally identifiable information (PII) by federal agencies. The E-Government Act of 2002 mandates Privacy Impact Assessments (PIAs) for all federal agencies when there are new collections of, or new technologies applied to, PII. The FOIA implements the principles that persons have a fundamental right to know what their government is doing. The Homeland Security Act of 2002 created the Chief Privacy Officer at DHS with responsibilities to ensure privacy and transparency in government are implemented throughout the Department, and was modified by the Implementing the Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), which gave additional authorities to the Chief Privacy Officer.

Due to the symbiotic relationship between privacy and FOIA, the Chief Privacy Officer is also the Chief FOIA Officer for the Department. The DHS Privacy Office manages and formulates the above statutory and policy-based responsibilities in a collaborative environment with DHS component Privacy Officers, Privacy Points of Contact (PPOCs),[2] and program offices to ensure

[1] The authorities and responsibilities of the Chief Privacy Officer were last 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. The 9/11 Commission Act added investigatory authority, the power to issue subpoenas, 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 responsibilities are further described on the DHS Privacy Office website: http://www.dhs.gov/xabout/structure/editorial_0510.shtm and in Section 4 of the previous Annual Report available at http://www.dhs.gov/xlibrary/assets/foia/privacy_rpt_foia_2008.pdf.

[2] A PPOC is an individual designated as responsible for privacy within their component, directorate, or major program, but is not generally a full-time privacy officer. Their privacy duties may be in addition to their primary

that all privacy issues receive the appropriate level of review and expertise. In addition, the DHS Privacy Office assures Department-wide statutory compliance with FOIA and the Privacy Act, as well as the consistent handling of disclosure requests.

The DHS 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 memorialized in *Privacy Policy Guidance Memorandum 2008-01*, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,*[3] released December 2008.[4] The FIPPs govern the appropriate use of PII at the Department. DHS uses the FIPPs to enhance privacy protections by assessing the nature and purpose of all PII collected to ensure it fulfills the Department's mission to preserve, protect, and secure the homeland.[5] Thus, the DHS Privacy Office applies the FIPPs to the full breadth and diversity of information and interactions within DHS. **Figure 2** illustrates how the FIPPs serve as a foundational framework for the various activities performed by the DHS Privacy Office to foster a culture of privacy throughout the Department.

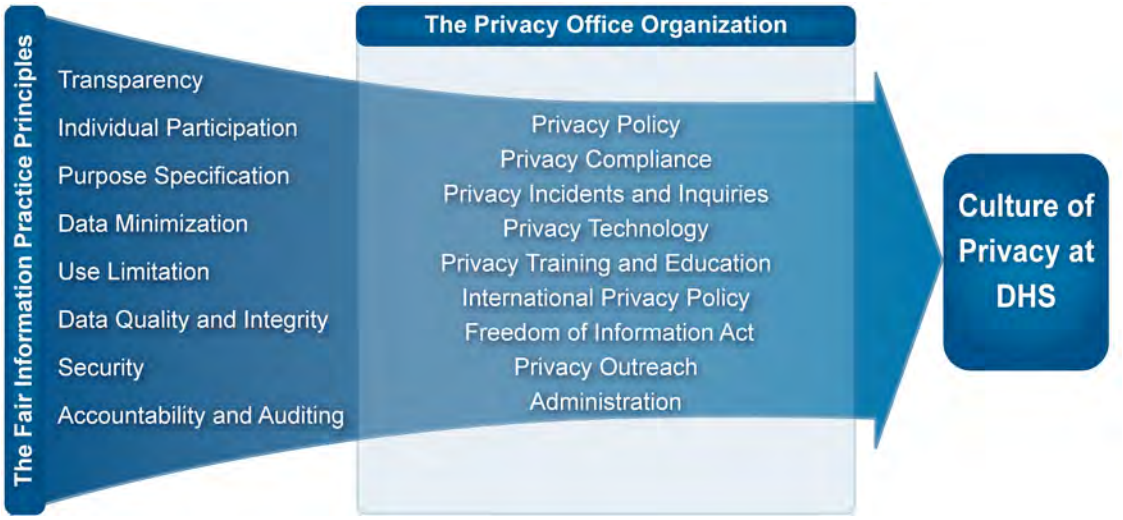


Figure 2: DHS Privacy Office Overview

B. Growth this year

The DHS Privacy Office continues to grow to support the increasing responsibilities and coordination required to fulfill the missions of both the Office and the Department. The DHS Privacy Office received an appropriation of $6.804 million in Fiscal Year (FY) 2009, an increase of $1.3 million (24%) over the FY 2008 enacted level, to support this additional growth. As of July 2009, the Office is comprised of 28 full-time equivalents, one DHS Fellow, two interns, and 12 contractors. During FY 2009, the DHS Privacy Office added the following new positions:

responsibilities. DHS has a network of PPOCs throughout the Department that works closely with component program managers and directly with the DHS Privacy Office to manage privacy matters within DHS.

[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[4] Privacy Policy Guidance Memorandum, Memorandum Number: 2008-1 (December 2008) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. See also Appendix XVI for more detailed discussion of the FIPPs.

[5] See Appendix A for a description of DHS's implementation of the FIPPs.

- Director, Privacy Incidents and Inquiries
- Associate Director, Policy and Education
- Associate Director, Privacy Technology and Intelligence
- FOIA Specialist (3)
- Privacy Compliance Specialist (1)
- Attorney-Advisor

In addition, the Office commenced the hiring process for a Senior Privacy Analyst, Associate Director of Communications, Associate Director of Privacy Compliance, Senior Attorney Advisor, and two Privacy Analysts during this reporting period. All hiring should be completed by the end of FY 2009.

The Office is converting contractor resources to recruit six FOIA Program Specialists to augment the FOIA staff. The additional FOIA staff members are needed to handle the substantial increase in FOIA requests, which have more than doubled since the White House Memorandum on FOIA and Transparency was issued on January 21, 2009.[6] The additional FOIA staff will enable the DHS Privacy Office to handle the high volume of FOIA and Privacy Act requests submitted in response to this new guidance.

The DHS Privacy Office received an allocation for a career Senior Executive Service (SES) Deputy Chief Privacy Officer in FY 2009. The Deputy Chief Privacy Officer served as the Acting Chief Privacy Officer from January 2009 until the appointment of the Chief Privacy Officer in March 2009. The addition of this SES position enables the DHS Privacy Office to continue to carry out its responsibilities effectively during times of transition.

The DHS Privacy Office will continue to promote growth in component privacy programs to address privacy requirements and enhance the culture of privacy throughout DHS. Component privacy staffing and support is discussed in Section III.D of this report.

[6] The DHS Privacy Office received 112 FOIA requests in June 2009, compared with 54 requests in January 2009.

II. Engaging the Public

The Chief Privacy Officer has made engaging the public a primary focus of her agenda for the DHS Privacy Office since her appointment in March 2009. The Office interacts with the public in a number of ways, many of which directly support the FIPPs in the areas of transparency and individual participation. These activities are critical to maintaining an open dialogue with the public, creating awareness about DHS Privacy Office operations, and reaffirming the Department's commitment to respecting the privacy rights of all people - both U.S. and international citizens. The following sections discuss the major areas in which the DHS Privacy Office engages with the public, specifically (1) providing individuals access to information through Privacy Act and FOIA requests (Transparency, Section II.A), (2) providing opportunities for redress when information must be corrected (Redress, Section II.B), and (3) informing the public about DHS activities and their impact on privacy (Public Education, Section II.C).

A. Transparency

The DHS Privacy Office supports the FIPPs' transparency principle through its handling of FOIA and Privacy Act requests. FOIA is the codification of the right to access records in the possession and control of federal agencies at the time a request is received. All agencies within the Executive Branch of the federal government are subject to the provisions of FOIA. The Act establishes a presumption that records in the possession and control of Executive Branch agencies are available to the public, except to the extent the records are subject to one or more of the Act's nine specific exemptions or three special law enforcement exclusions. On January 21, 2009, President Obama issued two important memoranda to the heads of Executive Departments and Agencies concerning government transparency. In the *Transparency and Open Government Memorandum for the Heads of Executive Departments and Agencies* (Transparency and Open Government Memorandum), he committed his administration to an "unprecedented level of openness in government,"[7] and in the *Freedom of Information Act Memorandum for the Heads of Executive Departments and Agencies* (FOIA Memorandum) he stressed the importance of the FOIA, stating that it is "the most prominent expression of a profound national commitment to ensuring an open government."[8] Consistent with President Obama's memoranda, FOIA requests are processed with a presumption of disclosure.

Perhaps most significantly, the Attorney General rescinded the October 12, 2001 Attorney General Memorandum on the FOIA and established a new standard for defending agency decisions to withhold information. When a FOIA request is denied, agencies will now be

[7] Transparency and Open Government Memorandum, 74 Fed. Reg. 4,685 (Jan. 21, 2009) available at http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf.
[8] FOIA Memorandum, 74 Fed. Reg. 4,683 (Jan. 21, 2009) available at http://edocket.access.gpo.gov/2009/pdf/E9-1773.pdf.

defended "only if (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions, or (2) disclosure is prohibited by law."[9]

The DHS Privacy Office is leading the Department's efforts to implement the sweeping policy changes required by President Obama's January 2009 FOIA memorandum, as well as the Attorney General's implementing guidance issued in March 2009.[10] The Disclosure and FOIA Group issued several types of guidance on implementing the new initiative. The Chief Privacy Officer also issued a memorandum to all DHS employees providing a general overview of FOIA and its importance in May 2009. The DHS Privacy Office drafted further guidance reminding employees of their responsibility to embrace this new era of openness and emphasizing the need for compliance with the Administration's policy of proactive disclosure. Lastly, the Chief Privacy Officer has discussed best practices and facilitated a dialogue among component FOIA offices related to the new Administration's guidance. Further efforts to guide the Department's execution of its responsibilities under FOIA are currently in development.

1. Freedom of Information Act

In accordance with Executive Order 13392, Improving Agency Disclosure of Information,[11] signed by President Bush on December 14, 2005, the Secretary designated the DHS Chief Privacy Officer to serve concurrently as the Chief FOIA Officer. The additional responsibility for disclosure compliance was delegated to the DHS Privacy Office in recognition of the close connection between privacy and disclosure laws. Given that FOIA is a pillar of the U.S. privacy protection framework, the Chief Privacy Officer's oversight of both privacy management and FOIA management allows for greater transparency of DHS operations. By policy, DHS implements both the FOIA and Privacy Act uniformly and consistently to provide maximum allowable disclosure of agency records upon request. Requests processed under the Privacy Act are also processed under FOIA; requesters are always given the benefit of the statute with the more liberal release requirements.

2. Intra-Departmental FOIA Compliance

During the reporting period, the Department continued working to merge the FOIA processes of multiple component agencies into a single FOIA program. Components actively participated in Department-wide FOIA initiatives to enhance responsibility and accountability, as well as to efficiently manage workload. For example, the Associate Director of Disclosure Policy and FOIA Program Development participated in a joint review of U.S. Customs and Border Protection's (CBP's) handling of requests for Passenger Name Record (PNR) data, along with the Director of Privacy Compliance, and the CBP PPOC and FOIA Officers. The Disclosure and FOIA Group also issued Department-wide guidance in Spring 2008 to ensure consistent responses to FOIA requests throughout DHS. The Department-wide guidance addressed the management of FOIA requests seeking agency records regarding ongoing law enforcement investigations and the treatment of DHS personnel information contained within agency records. Throughout the reporting period, the Disclosure and FOIA Group continued to advise Departmental components on implementation of this guidance.

[9] *Id.*
[10] The Attorney General's memo is available at http://www.usdoj.gov/ag/foia-memo-march2009.pdf.
[11] Exec. Order No. 13,392, Fed. Reg. 75,373 (Dec. 14, 2005).

In addition to policy and program development activities, the Disclosure and FOIA Group continued to process FOIA requests for the DHS Headquarters programs, including the Office of the Secretary. The Director of Disclosure and FOIA also served as a liaison to DHS Directorates and components, forwarding FOIA and Privacy Act requests seeking records they maintain. Additionally, the DHS Privacy Office offered FOIA and Privacy Act training to all DHS components on an as-needed basis to cultivate FOIA Officers' knowledge and expertise agency-wide.

3. Reducing FOIA Backlogs in DHS Components

The Disclosure and FOIA Group continued to address FOIA backlogs across the Department while improving efforts to manage the continuing increase of FOIA requests received by components. To support this effort, the Chief Privacy Officer is working with component leadership to ensure the Department's components devote adequate resources to their FOIA programs. During this reporting period, the Government Accountability Office (GAO) audited the Department's FOIA program and issued a report on March 20, 2009, entitled *Freedom of Information Act: DHS Has Taken Steps to Enhance Its Program, but Opportunities Exist to Improve Efficiency and Cost-Effectiveness*.[12] The report's key findings highlighted the Department's progress in decreasing its backlog by 24,048 requests (approximately 24%) between September 15, 2006 and October 17, 2008. GAO made recommendations to five of the seven operational components to encourage consistent implementation of technological enhancements, provide additional relevant training to DHS employees, and increase internal oversight of component FOIA programs. DHS concurred with GAO's recommendations, and the affected components immediately began addressing those recommendations with the support of the Chief Privacy Officer. The technological improvements recommended by GAO in the report have already been implemented in varying degrees by the components. Additionally, the DHS Privacy Office has worked with components to ensure consistent application of technological tools. The Chief Privacy Officer is confident these actions will have a substantial impact on the Department's FOIA processes, and that the components will continue to reduce their backlogs toward the Chief Privacy Officer's goal of zero. Further details about these initiatives will be provided in the *2009 FOIA Annual Report*.

In FY 2009, the Chief Privacy Officer focused on the DHS components with the largest backlog numbers, in particular, the U.S. Citizenship and Immigration Services (USCIS) FOIA program. The Disclosure and FOIA Group continued to assist USCIS design program improvements to reduce their backlog by increasing productivity. USCIS, which receives the greatest volume of FOIA requests in DHS, finalized a contract to obtain more FOIA personnel to help reduce the backlog. Between October 17, 2008 and June 30, 2009, several of the operational components were able to substantially reduce their FOIA backlogs. For example, USCIS reduced its backlog by 57%, from 70,175 to 30,167. Similarly, CBP reduced its backlog of overdue requests by 93%, from 2,198 to 163. Additionally, several components, including USCIS and ICE, implemented online tools for customers to access information pertaining to the status and location of their request in queue. USCIS also identified a number of FOIA requests that should

[12] http://www.gao.gov/products/GAO-09-260.

have been submitted and handled through the USCIS Genealogy Program,[13] thereby removing the requests from the FOIA processing backlog.

4. FOIA Outreach

In addition to the day-to-day interactions with the requester community, the Disclosure and FOIA Group meets regularly with representatives from the information access community, as well as immigration attorneys and advocates, in the course of processing access requests. For example, the Deputy Chief Privacy Officer, Senior Advisor, and Associate Director, Disclosure Policy and FOIA Program Development met with the American Civil Liberties Union (ACLU) in September 2008 to discuss matters related to both privacy and disclosure. The Chief Privacy Officer and Associate Director, Disclosure Policy and FOIA Program Development met with representatives of the American Immigration Lawyers Association (AILA) in May 2009 to discuss implementation of President Obama's new FOIA policies. The Associate Director, Disclosure Policy and FOIA Program Development also spoke at the 2009 American Society of Access Professionals (ASAP) annual conference to provide an overview of FOIA and discuss disclosure within the Department. Additionally, the Chief Privacy Officer was the keynote speaker at the American University Washington College of Law Symposium, Privacy Protection after Twenty Years under Reporter's Committee 2.0: The Freedom of Information Act in the Era of Obama.

B. Redress

Redress is a critical principle of the FIPPs and the Privacy Act, affording individuals the ability to request an update or correction to information maintained about them. Redress for U.S. persons is widely available. Due to the degree with which DHS interacts with members of the international community, the Department chooses to provide redress to non-U.S. persons in many of its programs under the DHS Mixed System Policy (i.e., policy on systems containing information about both U.S. and non-U.S. persons).[14] This section discusses the redress landscape at the Department and provides examples of major redress efforts currently supported by the DHS Privacy Office.

1. DHS Traveler Redress Inquiry Program (DHS TRIP)

In its second year of operations, the DHS Traveler Redress Inquiry Program (DHS TRIP)[15] continued to offer one-stop redress services to the public by providing a centralized processing point for individual travelers to submit redress inquiries. The public receives two important benefits through centralized redress request processing. First, the applicant is not required to know which component is responsible for addressing the request. In some cases, the agency or component with which the individual experienced the difficulty may not be the same agency or component whose information triggered the action. Consequently, DHS TRIP personnel review each case to determine which agency or component is involved and route the redress request to the appropriate agency or component. Second, DHS TRIP simplifies the redress process for

[13] The USCIS Genealogy Program is a fee-for-service program that provides family historians and other researches with access to historical immigration and naturalization records.
[14] Mixed Systems are discussed in more detail in Section II.B.4.
[15] Additional information about DHS TRIP is available at http://www.dhs.gov/files/programs/gc_1169676919316.shtm.

travelers. DHS TRIP enables multi-agency review of a case through a single application and interaction with the public. This process frees the applicant from the cost and burden of approaching each screening agency or component individually.

DHS TRIP acts in accordance with Department privacy policies and practices and was designed to seek only the minimum amount of PII necessary to process an applicant's request. Additionally, all DHS TRIP personnel have been trained to handle PII (including sensitive PII) and use Information Technology (IT) systems that have strong IT security safeguards.

In the coming year, DHS TRIP will be able to leverage the Secure Flight Program[16] to further streamline and improve the process of identifying travelers on the federal government's watch lists. Secure Flight will transfer the matching function of the No Fly and Selectee portions of the federal government's consolidated terrorist watch list from air carriers to the Transportation Security Administration (TSA) over the course of 2009. Among its many benefits, Secure Flight will allow the uniform prescreening of passenger information against federal government watch lists for domestic and international air travel. In addition, by mandating the collection of Full Name, Gender, and Date of Birth, it is expected that only a small fraction of travelers will be mistaken for individuals on the watch list. Consequently, travelers should experience fewer instances of additional screening due to misidentification, and reduce the need for redress through DHS TRIP.[17] While Secure Flight recently began implementation and only applies to a small number of passengers, early results already indicate that obtaining these additional data elements is indeed making a difference by permitting automated resolution of potential name matches to the watch list.

2. US-VISIT Redress Program

The US-VISIT program was established in March 2003 as one of the foundational programs within DHS. US-VISIT was created to accurately record the entry and exit of travelers to the U.S. by collecting biographic and biometric information (e.g., digital fingerprints and photographs). Today, US-VISIT is advancing the security of the U.S. and worldwide travel through information sharing and biometric solutions for identity management. See Section XI.I for additional information about US-VISIT.

One of the goals of the US-VISIT redress program is to provide a mechanism by which erroneous personal information can be corrected to prevent future inconvenience or hardship to legitimate travelers entering the U.S. US-VISIT's redress process affords individuals the opportunity to receive a fair, timely, and independent review of issues or concerns regarding the collection and use of their biometrics to enter the U.S. A robust redress program helps maintain the integrity of the information US-VISIT collects and ensures travelers that the information maintained about them is accurate, complete, and current. Individuals with a complaint or concern regarding delayed or denied airline boarding, delayed or denied entry into and/or exit from the U.S., and/or being continuously referred to additional (secondary) screenings may submit a redress request. Redress requests may be submitted via mail, fax, email, and since 2007, through the DHS TRIP program. US-VISIT's goal is to provide a timely response to all

[16] See Section IX.E.4 for more information regarding the Secure Flight Program.
[17] Misidentification refers to individuals who have names and personal information similar to a record in the watch list.

redress requests within 22 days. US-VISIT received and handled 635 redress requests during FY 2009, responding on average within 15 days of receipt of the request.

3. Transportation Sector Threat Assessment and Credentialing Redress

TSA's Office of Transportation Threat Assessment and Credentialing (TTAC) conducts security threat assessments and completes adjudication services in support of TSA's mission to protect U.S. transportation systems from individuals that may pose a threat to transportation security. TTAC provides daily checks on over 8.5 million transportation sector workers against the consolidated federal watch list. TTAC provides a redress process that includes both appeals and waivers for transportation sector workers who feel that they were wrongly identified as individuals who pose a threat to transportation security. Typical redress requests have involved documentation missing from initial submissions, immigration issues, or requests for waivers of criminal histories. Over the past year, TTAC granted 43,085 and denied 245 appeals. Additionally, TTAC granted 2,207 and denied 41 waivers.

4. Mixed System Policy

As a matter of law, the Privacy Act provides statutory privacy rights to U.S. citizens and Legal Permanent Residents (LPRs), collectively known as U.S. persons. DHS extends the Privacy Act's protections to non-U.S. persons for information collected, used, retained, and/or disseminated by DHS in mixed systems (i.e., systems that contain information on both U.S. and non-U.S. persons), as set forth in the DHS Privacy Office *Privacy Policy Guidance Memorandum Number 2007-1 Mixed System Policy* (DHS Mixed System Policy).[18] The DHS Mixed System Policy states that 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, LPR, visitor, or alien. Under this policy, DHS components handle non-U.S. person PII held in mixed systems in accordance with the DHS FIPPs. This directly supports the FIPPs principle of individual participation, which calls for appropriate redress in such scenarios.

As the Privacy Act does not cover visitors and aliens, some international government officials have questioned whether the U.S. provides effective privacy protection and redress options for their citizens. Questions most frequently arise in the context of border protection systems that impact international travelers. For the reporting period, the Privacy Office continued efforts to educate the public, particularly international government officials, of redress options available when individuals believe the Department has inaccurate data or has misused the data held within DHS systems.

At the Secretary's direction, the Chief Privacy Officer conducted outreach specifically focused on redress during two trips to the European Union (EU). She had bilateral discussions with the EU and officials in France, Belgium, Germany, Sweden, the UK, and the Netherlands. In an effort to reach the European public, she conducted an interview with the EU's *Parliament Magazine*, recorded a series of video press releases through the United States Mission to the European Union, and published an article in the British publication *Data Protection Law &*

[18] The DHS Mixed System Policy, initially issued on January 19, 2007, was revised on January 7, 2009. It is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

Policy.[19] The article provided a discussion of redress options available in the U.S. and was written to increase international understanding of U.S. and DHS privacy practices. The DHS Privacy Office is currently seeking further information on oversight mechanisms covering security service use of commercially-collected information in the EU and its Member States.

This outreach sought to correct the misperception that the Privacy Act represents the only form of relief available to the public. The DHS Privacy Office has also been providing education internally that the Department affords visitors to the U.S. the same administrative protections it is required to provide to U.S. citizens under the DHS Mixed System Policy. Visitors have full access rights under FOIA (including judicial review) and may seek correction of records under DHS TRIP or a direct appeal to the Chief Privacy Officer. Other avenues for effective redress may also be available depending on the situation, including prosecution under the Computer Fraud and Abuse Act (CFAA), the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Internal Revenue Service Code, and other laws.

In December 2008, the Chief Privacy Officer issued an *Interim Report on the EU Approach to the Commercial Collection of Personal Data for Security Purposes: The Special Case of Hotel Guest Registration Data,*[20] highlighting the need for further information about redress options available to U.S. citizens in the EU and its member states.

C. Public Education

1. Privacy Advocacy Community

Throughout this reporting period, the Chief Privacy Officer engaged in information exchanges with the privacy advocacy community to ensure they are well informed about DHS programs and projects that may pose particular privacy concerns. Upon her appointment, the Chief Privacy Officer began a series of introductory outreach meetings with advocacy groups to begin a relationship of open dialogue and to demonstrate that she is interested in hearing their concerns. In addition, the Chief Privacy Officer has begun holding quarterly open meetings with the privacy advocacy community. These meetings, called Privacy Information for Advocates meetings, are intended to brief the advocacy community on the work of the DHS Privacy Office and provide a forum for the privacy advocacy community to express feedback or concerns to the Chief Privacy Officer and the Department. The first meeting was held in June 2009, with future meetings scheduled in September and December 2009, and March 2010. Other outreach efforts included briefings on programs such as TSA's Whole Body Imaging Program, NPPD's Comprehensive National Cybersecurity Initiative (CNCI), and the REAL ID Program.

To supplement these face-to-face meetings, the DHS Privacy Office makes efforts to alert the privacy advocacy community by email when new reports or privacy documents of major importance are released. In addition, the Office periodically disseminates a newsletter, *Privacy Matters,* designed to highlight Office activities. The DHS Privacy Office views the privacy advocacy community as an important resource for policy development and invites them to bring their concerns and expertise to the attention of the Office.

[19] In June 2009, the Chief Privacy Officer published *Finding Relief for Privacy Infringements in the New World* in Data Protection Law & Policy, a UK publication. The article is available at http://www.e-comlaw.com/dplp/details_contents.asp?ID=621.
[20] http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_hotel_int.pdf.

2. Public Workshops

The DHS Privacy Office periodically hosts public workshops to explore relevant privacy topics and issues and discuss them in an open forum. On June 22-23, 2009, the DHS Privacy Office held a public workshop entitled Government 2.0: Privacy and Best Practices. This workshop is discussed in detail in Section VIII.A.

3. International Education

One of the DHS Privacy Office's goals is to promote international understanding about how privacy is relevant to the Department's mission and operations. Increasingly, foreign audiences are asking the DHS Privacy Office to demonstrate how the Department incorporates into practice the principles articulated in international guidelines, such as the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines and the Asia Pacific Economic Cooperation (APEC) Privacy Framework, as well as those memorialized in U.S. law, directives, and policy statements. By making presentations regarding how the Department operationalizes privacy, the DHS Privacy Office increases confidence in Department programs and demonstrates U.S. leadership on applying privacy in government programs – an area where many governments are looking for best practices.

During the reporting period, the DHS Privacy Office continued its program of inviting foreign officials to exchange personnel and attend a full week of internal and external briefings arranged by the Office. Over three separate exchange programs, the DHS Privacy Office hosted delegates from the Spanish Data Protection Authority, the United Kingdom (UK) Ministry of Justice and Information Commissioner's Office (ICO), the German Ministry of the Interior, the Mexican Institute for Federal Access to Information, and the European Commission. In addition, the DHS Privacy Office's Director of Compliance and Associate Director for International Privacy Policy were hosted by the UK ICO for a week of meetings about privacy oversight, which included discussions with the Ministry of Justice, Cabinet Office, and UK Borders Agency. The exchanges were an effective means of promoting the principle of reciprocity and fostering the trust necessary for sharing vital information with ease, security, and transparency. The DHS Privacy Office will continue this program in FY 2010.

The DHS Privacy Office accepted invitations to provide presentations to the Mexican Senate and French Senate to discuss best practices for embedding privacy principles into the work of the public sector. The DHS Privacy Office provided overviews of the U.S. government's privacy framework and its specific application to DHS. The Chief Privacy Officer met with the following representatives of foreign governments who were visiting the U.S. to discuss various privacy matters: Mr. Max-Peter Ratzel, Director of Europol; Dr. Dieter Wiefelspuetz, German Member of Parliament; Mr. Peter Schaar, German Federal Data Protection Commissioner; Dr. Anne Cavoukian, Information and Privacy Commissioner for Ontario; Ms. Jennifer Stoddart, Privacy Commissioner of Canada; Mr. Richard Thomas, UK Information Commissioner; Peter Hustinx, European Data Protection Supervisor; Dr. Artemi Rallo Lombarte, Director of the Spanish Data Protection Agency; and Ms. Karin Riis-Jordensen, Danish Member of the European Parliament and Chair of the European Privacy Association.

Throughout the reporting period, the DHS Privacy Office participated in conferences hosted by international privacy organizations and policy groups, such as the 2008 meeting of the International Conference of Data Protection and Privacy Commissioners, the March 2009

meeting of the International Working Group on Data Protection in Telecommunications (Berlin Group), the NatSec '08 Conference in Brussels, the University of Utrecht's symposium on privacy in the fight against terrorism, the ID World Conference in Milan, the Duke University Data Protection Day Conference, an Interdisciplinary Conference on Current Issues in IT Security at the Max Planck Institute in Freiburg, an event hosted by the Migration Policy Institute, and the European e-Identity Conference in London. By participating in multiple events in a diversity of locations, the Privacy Office achieves the Secretary's goal of broad international engagement.

4. DHS Privacy Office Website

The DHS Privacy Office continues to use its website (http://www.dhs.gov/privacy) as a primary means of sharing information with the public. The website enables members of the public to sign up to receive email alerts whenever the website's privacy compliance documentation or reports and guidance sections are updated. Examples of information added during this reporting period include the following:

- The *Privacy and Civil Liberties Guidance Memorandum regarding the DHS Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy* (DHS ISE Privacy and Civil Liberties Protection Policy);[21]
- A *DHS Data Privacy and Integrity Advisory Committee* (DPIAC) *White Paper on DHS Information Sharing and Access Agreements*;[22]
- The agenda, public comments, and transcript for the Government 2.0: Privacy and Best Practices workshop;[23]
- A DHS report regarding PNR data and protection information;[24]
- The *2008 DHS Privacy Office Annual Report to Congress*;[25]
- New PIAs and System of Record Notices (SORNs); and
- Departmental FOIA Directives and Instructions.[26]

The Chief Privacy Officer will continue to refine and enhance the user experience of the website during the next reporting period.

[21] http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.
[22] http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_issa_final_recs_may2009.pdf.
[23] http://www.dhs.gov/xlibrary/assets/privacy/privacy_gov20_June2009_agenda.pdf.
[24] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.
[25] http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2008.pdf.
[26] http://www.dhs.gov/xfoia/editorial_0424.shtm.

III. Collaboration: Within and Outside DHS

The DHS Privacy Office engages with many individuals, groups, and agencies both inside and outside of the Department. These relationships help support the DHS Privacy Office in achieving its mission to educate others about the Office's activities and responsibilities, and contribute to the broader federal privacy community. Internal DHS offices, federal agencies, and international ministry and data protection counterparts all play an important role in the collaboration efforts of the Department. Several of these efforts are discussed in the following sections.

A. 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 [CRCL] to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner." The CRCL has a matching obligation in section 705 to coordinate efforts with the Chief Privacy Officer.

The DHS Privacy Office and CRCL continued to work closely during the reporting year on a wide variety of DHS programs including, but not limited to, cybersecurity, information sharing, intelligence product review, E-Verify, Real ID, and a number of other programs. The two offices held bi-weekly teleconferences to discuss issues of common concern, a practice that was initiated during the previous reporting period. The two offices also worked closely together in support of the DHS State and Local Fusion Center Program. For the second straight year, the DHS Privacy Office and CRCL co-hosted a booth at the National Fusion Center Conference in Kansas City, Missouri. The two offices also continued their close collaboration to develop and deliver training to state and local fusion centers across the U.S.

On June 5, 2009, the DHS Privacy Office and CRCL issued their first joint policy document. The DHS ISE Privacy and Civil Liberties Protection Policy[27] was developed and signed by both the Chief Privacy Officer and Acting Officer for CRCL in response to a requirement established by the President's Program Manager for the Information Sharing Environment (ISE). Both offices anticipate further cooperation during the next reporting year as the Department takes steps to implement this new policy.

In addition to these ongoing projects, the DHS Privacy Office and CRCL worked on the planning of the National Immigration Information Sharing Operation (NIISO) to certify that the program will comply with all applicable privacy and civil liberties standards as required by the 2008 Omnibus Appropriations Act. NIISO is the program by which the Office of Intelligence and Analysis (I&A) will receive, research, and respond to requests from participating intelligence and law enforcement-related agencies for DHS-held immigration-related information. The DHS

[27] http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.

Privacy Office and CRCL accompanied NIISO staff on site visits to USCIS immigration information facilities and coordinated efforts to develop the program's PIA and Civil Liberties Impact Assessment (CLIA). The offices will continue to work in close cooperation to publish the PIA and CLIA for NIISO in the next reporting year.

B. 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), federal agencies must establish a DIB to oversee and approve their use of computer "matching programs." 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.[28]

Before the Department can match its data with data held by 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.

Under the terms of the computer matching provisions of the Privacy Act, CMA may be established for a term of 18 months. Provided there are no material changes to the matching program, existing CMAs may be recertified once for a period of 12 months. Thus, the Department must re-evaluate the terms and conditions of even long-standing computer matching programs regularly.

During the reporting period, DHS entered into five 18-month CMAs, formally re-establishing long-standing computer matching programs between USCIS Systematic Alien Verification for Entitlements program and the following state parties:

- The Massachusetts Division of Unemployment Assistance;
- The New Jersey Department of Labor and Workforce Development;
- The New York State Department of Labor;
- The Texas Workforce Commission; and
- The California Department of Healthcare Services.

The state parties estimated that the matching programs will reduce fraudulent benefit payments, resulting in an aggregated savings of over $20 million during the 18-month agreement period.

During the reporting period, DHS also recertified one Computer Matching Agreement between USCIS/ICE and the Social Security Administration (SSA) for a period of 12 months.

[28] 5 U.S.C. § 552a(a)(8)(i)(1).

C. Office of the Chief Information Security Officer

Throughout the year, the DHS Privacy Office coordinated with the Office of the Chief Information Security Officer (CISO) on a number of projects.

The DHS Privacy Office participated in DHS Chief Information Officer (CIO) meetings held twice a month, as well as monthly Compliance Working Group meetings run by CISO. During these meetings, the Office provided updates regarding privacy training initiatives and projects that may require the participation of, or be of interest to, the DHS CIO, the DHS CISO, and/or the component CISOs. The DHS Privacy Office was also able to gain a better understanding of systems being considered for development, planned and proposed changes to existing systems, systems being retired, information changes, and updates to information security policies and procedures that could impact privacy (e.g., updates and changes to DHS Directive 4300A – Sensitive Systems Policy). Participation in these meetings ensures that privacy and security are addressed in unison and promotes efficiency and coordination among the CIO, the CISO and the DHS Privacy Office.

In addition to attending CIO and CISO meetings, the DHS Privacy Office works with the CISO's Office to draft and implement privacy documentation. For example, the DHS Privacy Office undertook the drafting of a proposed DHS guide for managing computer-readable extracts (CREs) from DHS systems containing sensitive PII. The Office provided drafts of the proposed CRE guidance to the CISO's Office and component Information Systems Security Managers, as the CRE guidance document delegates responsibility for managing CREs to system owners and data owners. Obtaining input from both the CISO's Office and component ISSMs were critical to ensure a coordinated and seamless implementation of the guidance. The DHS Privacy Office also worked with the CISO Office to incorporate edits into the DHS Directive 4300A to reflect new policies and procedures outlined in the proposed CRE guidance document.

The DHS Privacy Office also participates in the larger coordination work of Department-wide information technology management with the OCIO through twice monthly meetings of the DHS CIO Council, where the DHS Privacy Office benefits from hearing about issues and challenges facing the Department in that area.

D. International Coordination within DHS

The Department's cross-border efforts involve information sharing with foreign governments and regional organizations. The DHS Privacy Office supports senior leadership and component offices engaged in these activities. Examples of DHS Privacy Office coordination within the Department during the reporting period are as follows:

- Providing input into US-VISIT's agenda for hosting of European Members of Parliament interested in biometric entry and exit programs;
- Assisting the Screening Coordination Office and the Office of International Affairs (OIA) with responses to questions from the EU concerning the Electronic System Travel for Authorization (ESTA), an automated system that assists in determining and notifying individuals of eligibility to travel to the U.S. under the Visa Waiver Program (VWP);

- Providing guidance on the legal, privacy, and governance challenges to information sharing within the Five Country Conference, which includes Australia, Canada, New Zealand, the United Kingdom, and the United States;
- Providing the Director of US-VISIT with talking points for an event hosted by the Migration Policy Institute;
- Reviewing the efforts of CBP and the DHS Office of Policy to fully implement the provisions of the Agreement between the U.S. and EU on PNR data and the representations in the Automated Targeting System (ATS) System of Record Notice (SORN);and
- Contributing to development of documentation on international data sharing for the Intergovernmental Consultations on Migration, Asylum and Refugees, submitted by the Office of International Affairs.

E. Development of Component Privacy Offices

1. DHS Memo: Designation of Component Privacy Officers

In June 2009, the Deputy Secretary issued a memorandum to component heads directing certain components to designate a senior level federal employee as a component Privacy Officer. The memorandum further states that these individuals will serve as the primary point of contact for the DHS Privacy Office, must have a background in privacy, and should receive adequate resources to complete their duties effectively. The duties of component Privacy Officers are also defined in the memo. The following components are expected to have a Privacy Officer by early October 2009 as stated in the memo:

- Federal Emergency Management Agency (FEMA);
- National Protection and Programs Directorate (NPPD);
- Office of Intelligence and Analysis (I&A);
- Science and Technology Directorate (S&T);
- Transportation Security Administration (TSA);
- U.S. Citizenship and Immigration Services (USCIS);
- U.S. Coast Guard (USCG);
- U.S. Customs and Boarder Protection (CBP);
- U.S. Immigration and Customs Enforcement (ICE); and
- U.S. Secret Service (USSS).

Prior to the memorandum, several components had Privacy Officers and privacy programs in place that met the criteria defined in the memorandum. The Deputy Secretary's memorandum solidifies privacy at an operational level throughout DHS components and offices that collect, use, and store PII. The appointment of component Privacy Officers will expand and systematize the culture of privacy in DHS.

2. Building the Privacy Compliance Network

As mentioned earlier in this report, the DHS Privacy Office has diligently worked to develop a network to support privacy generally, and privacy compliance specifically, within DHS.

Without this existing network, the privacy compliance process would be significantly hampered. Upon beginning her tenure, the Chief Privacy Officer engaged in a series of outreach meetings with component heads throughout the Department. These meetings allowed the Chief Privacy Officer to address the importance of privacy with the heads of the components, thus supporting the Compliance Group's effort to strengthen privacy awareness and education and further bolstering the network of support for privacy.

During the reporting period, the Compliance Group also continued to hold monthly meetings with component Privacy Officers and PPOCs to discuss compliance issues and discuss areas of similar concern. These meetings continue to serve a critical support function in coordinating and managing privacy efforts across the Department. Additionally, the Compliance Group began holding quarterly off-site meetings with the component Privacy Officers and PPOCs to further strengthen the relationship between the component offices and the DHS Privacy Office. Component Privacy Officers and PPOCs discussed cross-cutting privacy issues, common privacy policies, and solutions during these quarterly Privacy Officer Meetings. The meetings provided an environment for component Privacy Officers and PPOCs to collaborate with each other, as well as the DHS Privacy Office's Compliance staff, to discuss and address important privacy issues.

F. Collaboration within the Federal Government

1. Federal Chief Information Officers Council's Privacy Committee

One of the ways in which the DHS Privacy Office plays a key leadership role defining privacy policy and practice across the federal government is through its active participation on the Privacy Committee of the Federal Chief Information Officers Council (Federal CIO Council). The Federal CIO Council was first established by Executive Order in 1996 and then codified into law by Congress in the E-Government Act of 2002. Comprised of Senior Agency Officials for Privacy and Chief Privacy Officers across the federal government, the Privacy Committee was established in 2008 to serve as the principal interagency forum to improve agency practices for the protection of privacy. The DHS Chief Privacy Officer was asked to serve as a co-chair of the Privacy Committee in April 2009. In addition to the Chief Privacy Officer's leadership role, senior members of the DHS Privacy Office serve as co-chairs of the Privacy Committee's Best Practices Subcommittee and the International Subcommittee.

One of the Privacy Committee's most significant accomplishments within its first year of establishment was holding the first Federal Privacy Summit on October 23, 2008. The Federal Privacy Summit was a one-day conference for employees across the federal government working in the area of privacy. The Privacy Committee plans to hold this conference annually, and the DHS Privacy Office staff intends to continue to play a key role in the planning of the event and as speakers. Other Privacy Committee activities include coordinating with the Federal CIO Council to ensure that privacy is addressed within its information technology projects and serving as a resource to the Office of Management and Budget (OMB) on privacy-related matters.

The Privacy Committee formed the International Subcommittee in 2009 as a forum to discuss developments in global privacy policy. The Subcommittee's objectives are to facilitate coordination among federal agencies that participate in international privacy organizations,

increase consultation among interested agencies, develop a consistent international data privacy strategy, and deliver a coherent U.S. Government message at international fora.

As part of its leadership on federal privacy policy, the DHS Privacy Office co-chairs the International Subcommittee with the Department of State. The DHS Privacy Office also co-chairs the Best Practices Subcommittee of the Privacy Committee, which is working on several interagency projects to define privacy best practices for OMB's Federal Enterprise Architecture and the Federal E-Authentication initiative to enable federal websites to recognize email addresses and other identifiers used by third parties.

The DHS Privacy Office also actively participates on the Web 2.0 Subcommittee of the Privacy Committee. The subcommittee provided a forum for discussion and recommendations on how best to promote President Obama's Open Government and Transparency initiative while protecting privacy. Similar to the issues federal agencies first faced when creating federal websites, agencies must now develop policies and processes that ensure that the use of social media, which is designed to increase public participation in government, is consistent with privacy law and regulations and does not erode privacy. The subcommittee provides a vehicle to advise OMB on privacy issues associated with social media.

2. Information Sharing Environment and Privacy Guidelines Committee

DHS is a key participant in the ISE. The Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA) created the ISE to facilitate the means for sharing terrorism information among all appropriate federal, state, local, and tribal entities, as well as the private sector. As directed in IRTPA, the President issued a *Memorandum to the Heads of Executive Departments and Agencies regarding Guidelines and Requirements in Support of the Information Sharing Environment*,[29] 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:

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

[29] http://www.ise.gov/docs/Memo_on_Guidelines_and_Rqmts_in_Support_of_the_ISE.pdf.

The DHS Privacy Office continues to support the implementation of the ISE—particularly the fifth guideline related to the protection of privacy—both within the Department and government-wide.

Of particular significance this year, the Department met one of the critical deliverables required of ISE participants with the publication of the DHS ISE Privacy and Civil Liberties Protection Policy, jointly issued by the DHS Privacy Office and CRCL on June 5, 2009. In the coming year, the DHS Privacy Office and CRCL will deliver training based on the new policy. The policy is discussed in more detail in Section V.A of this report.

At DHS, the Chief Privacy Officer sits as an ex officio member of the Information Sharing Governance Board (ISGB). The ISGB is the Department's senior-level board responsible for overseeing the vast portfolio of DHS information sharing programs. The Chief Privacy Officer's presence ensures that privacy is considered throughout the development cycle of each information sharing activity undertaken by the Department. During the reporting year, the ISGB amended its charter, adding component heads to the board and inviting the Officer for CRCL to attend meetings as an additional ex officio member. The IGSB also endorsed the Shared Mission Community (SMC) framework for identifying and resolving information sharing issues unique to particular DHS missions and approved the creation of an Intelligence SMC, which joined the previously established Law Enforcement SMC.

The DHS Privacy Office staff also served as Action Officers on the Department's Information Sharing Coordination Council (ISCC). The ISCC is a working group of the ISGB and is comprised of representatives from across the Department. It was established to assist the ISGB and further ensure coordinated Department-wide positions regarding information sharing areas such as data calls, data analysis, strategy development, implementation of recommendations, and feedback. The ISCC also formed Integrated Project Teams (IPTs) and Working Groups (WGs) as needed to resolve specific information sharing issues and develop policy recommendations for further consideration. A representative of the DHS Privacy Office served as the co-chair of the ISCC IPT to revise the Department's Guidance on Information Sharing Access Agreements (ISAA). In this role, the DHS Privacy Office representative worked with the ISCC IPT to begin establishing template language that addresses privacy issues, assists users of the guidance to identify privacy concerns, and ensures information sharing agreements are properly reviewed for consistency with federal privacy law and DHS privacy policy.

The DHS Privacy Office also served as a co-chair of the interagency Privacy Guidelines Committee's (PGC's) State and Local Working Group (SLWG). The SLWG issued a set of recommendations for fusion centers that were adopted by the PGC and later became part of the *Baseline Capabilities for State and Major Urban Area Fusion Centers September 2008: A Supplement to the Fusion Center Guidelines*[30] (Baseline Capabilities) document, issued by the Global Justice Information Sharing Initiative (Global). Global's products are released jointly by DHS and the Department of Justice's (DOJ's) Bureau of Justice Assistance and are widely utilized by fusion centers across the U.S. to improve their intelligence and information sharing capabilities. The Chief Privacy Officer also contributed to the national effort to establish information sharing policies that address privacy considerations and has served on the PGC since it was established by the Program Manager for the Information Sharing Environment (PM-ISE).

[30] http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

In FY 2009, the Chief Privacy Officer accepted an invitation from the PM-ISE to serve as one of the tri-chairs of the interagency PGC.

The DHS Privacy Office continued to support implementation of the PGC's Privacy Guidelines by all ISE participants at the federal, state, and local level. On April 27, 2009, for instance, a representative of the DHS Privacy Office participated in a panel before a plenary session of the National Forum on Information Sharing in Washington DC entitled An Undivided Mission: Civil Rights, Civil Liberties, and Privacy in the Information Sharing Environment. The Chief Privacy Officer and Office staff participated in a number of other events in support of this effort, such as the Governors Homeland Security Advisors Council and the 2009 National Fusion Center Conference, which are covered more extensively throughout this report.

G. Collaboration Abroad

The DHS Privacy Office International Privacy Policy (IPP) group, led by the Co-Directors of International Privacy Policy, is an integral part of the Department's international engagement efforts. Through participation in multilateral organizations, the DHS Privacy Office promotes dialogue with foreign partners about the core ideals that underlie the Privacy Act. The DHS Privacy Office supports the Department's negotiation and implementation of cross border information sharing programs by explaining to foreign partners the means by which DHS protects the privacy rights of U.S. and non-U.S. citizens while meeting its goals and objectives.

1. Participation in International Privacy Groups

The DHS Privacy Office, together with the U.S. Federal Trade Commission (FTC), continued as official observers to the International Conference of Data Protection and Privacy Commissioners (ICDPPC). Led by the Spanish Data Protection Authority in 2009, this organization is developing "universally accepted international privacy standards" for broad adoption by the private and public sectors. The DHS Privacy Office and the FTC attended two meetings organized by Spain and developed an interagency-cleared U.S. position on the draft standard. Spain will present a final document for adoption at the ICDPPC meeting in Madrid in November 2009.

The DHS Privacy Office also continued to contribute to the OECD's Working Party on Information and Privacy (WPISP). The Office is particularly interested in the WPISP's Global Privacy Dialogue initiative, and succeeded in having the DHS Privacy Office Government 2.0 Workshop[31] recognized as an input to the Global Privacy Dialogue. The Global Privacy Dialogue will conclude with a conference commemorating the 30th anniversary of the OECD Privacy Guidelines. The DHS Privacy Office hopes to have a role in the planning and execution of the conference as appropriate.

The International Organization for Standards (ISO), an internationally recognized standards development body, continued development of non-technical privacy standards. During the reporting period, the IPP group formally joined the technical advisory group to the American National Standards Institute (ANSI), the U.S. representative to the ISO. The DHS Privacy Office also participates in an ISO task force to re-examine the issue of privacy and the steps

[31] See Section VIII.A for information regarding the Government 2.0 Workshop.

undertaken by this technical body. The Office coordinated with the Department of Commerce and consulted with the FTC during its work with ISO.

The DHS Privacy Office continued to participate in the Asia Pacific Economic Cooperation's Data Privacy Subgroup through contributions to the interagency delegation. During the year, the Office reviewed and commented on upcoming meeting agendas and work plans for the E-Commerce Subgroup Data Privacy Subgroup.

2. Cross -border Information Sharing

As the Department negotiated and implemented information sharing agreements with foreign partners, the DHS Privacy Office explained the U.S. Government privacy framework and the tools used to provide transparency and accountability for the proper handling of personal information. One of the most important efforts in cross-border information sharing with the EU was the Office's participation in the High Level Contact Group (HLCG). Since November 2006, DHS together with the Departments of State and Justice engaged in discussions with the European Council Presidency and European Commission to identify "common principles" of an effective regime for privacy protection. The HLCG issued a joint report in December 2008 acknowledging the shared goal of a binding international agreement based on the "common principles." The HLCG made significant progress during the reporting period and the DHS Privacy Office hopes to begin work on the binding international agreement in FY 2010.

The DHS Privacy Office also supported information sharing with Canada. The Office reviewed and provided comments to CBP's Memorandum of Understanding (MOU) with Canada's Border Services Agency regarding the use, disclosure, and storage of Canadian Enhanced Driver's License (EDL) information. In response to a request from the Department's Ontario attaché, the DHS Privacy Office engaged in a teleconference with members of the Canadian press to respond to concerns with EDLs. The Office also engaged with the Office of International Affairs, CBP, and the Department of State in the ongoing negotiation of the U.S.-Canada MOU on visa information sharing.

The Preventing and Combating Serious Crime (PCSC) Agreements, which allow for the exchange of biometric and biographic data and are required of all Visa Waiver Program countries under the 9/11 Commission Act, are a significant advancement in cross border information sharing. These agreements are based on the PCSC agreement with Germany signed in FY 2008. The DHS Privacy Office partnered with the OIA, DOJ, and the Department of State to explain the U.S. privacy framework to foreign governments deliberating the agreements.

H. Data Privacy and Integrity Advisory Committee (DPIAC)

The DHS DPIAC is chartered under the Federal Advisory Committee Act (FACA),[32] as amended, to provide advice to the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII, data integrity, and other privacy-related matters. DPIAC members serve as Special Government Employees and represent a balance of interests on privacy matters from academia, the private sector (including for-profit and not-for profit organizations), and the privacy advocacy community. The Committee undertakes matters assigned to it by the Chief

[32] Federal Advisory Committee Act, 5 U.S.C. app.

Privacy Officer, and conducts its deliberations in public meetings. Its role is advisory only. The DPIAC issues its findings and recommendations in public reports. These reports, and DPIAC meeting agendas and transcripts, are available on the DHS Privacy Office website.

During the reporting period for this report, the DPIAC held five public meetings and issued four public reports. Information about the DPIAC, meeting agendas, transcripts, reports, and recommendations are posted on the DHS Privacy Office website.

On September 17, 2008, the DPIAC held a public meeting in Las Vegas, Nevada. After the Chief Privacy Officer opened the meeting, the DPIAC received a series of briefings from the newly appointed component Privacy Officers and PPOCs from ICE, CBP, USCIS, FEMA, USCG, and US-VISIT. The next two panels focused on privacy and programs within S&T, particularly within the directorate's physical screening research. The last briefing, delivered by an IBM Distinguished Engineer and Chief Scientist and member of the Markle Foundation Task Force on National Security in the Information Age, focused on technology and privacy. During the meeting, the DPIAC members deliberated on proposed recommendations and adopted a report entitled *Recommendations on Addressing Privacy Impacts in Department of Homeland Security Grants to State, Local, and Tribal Governments and other Organizations*. The report recommends that DHS require prospective grantees to provide information on their handling of PII to address privacy impacts in the DHS grant-making process. While in Las Vegas, the DPIAC members toured the McCarron International Airport where they observed a demonstration of the use of radio frequency identification (RFID) technology to route passenger baggage. They heard a briefing on theft and cheating in the gaming industry, strategies for combating cheating, and the privacy implications of such strategies. Lastly, the DPIAC visited the surveillance room of a casino for a demonstration of how casinos use closed circuit television (CCTV) to monitor activities of customers and staff on the gaming floor. These site visits provided the DPIAC with practical insights into the privacy impact of utilizing technologies like RFID and CCTV, which are also used in various homeland security initiatives.

The DPIAC's next public meeting was held on December 3, 2008, in Arlington, Virginia. In his opening remarks, the Chief Privacy Officer thanked the DPIAC members for their service during his tenure. The Committee then turned its attention to the Presidential Transition and setting a privacy agenda for the incoming Secretary of Homeland Security and new Chief Privacy Officer. The DPIAC heard a presentation by a member of the DHS Transition Team, as well as a panel comprised of members of the privacy advocacy community. The DPIAC also heard a briefing on the U.S. Government-wide cybersecurity initiative. The DPIAC ended the meeting with subcommittee updates, which included briefings from the ad hoc subcommittees on E-Verify and the Presidential Transition. Following the subcommittee briefings, the DPIAC members deliberated on a draft report developed by the ad hoc subcommittee on E-Verify and adopted a set of recommendations that appear in the DPIAC report entitled *Options for Verifying the EIN or Otherwise Authenticating the Employer in the E-Verify Program* (Report No. 2008-02) (E-Verify Report).[33] The E-Verify Report makes seven specific recommendations to the Secretary of Homeland Security and the Chief Privacy Officer for addressing privacy and data security risks associated with the identification and authentication processes for employers using the Department's E-Verify system.

[33] http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_e_verify_12-2008.pdf.

On February 3, 2009, the DPIAC met by public teleconference to deliberate and vote on a draft letter to the new Secretary of Homeland Security and DHS Chief Privacy Officer including recommendations for the new Administration on DHS Privacy Office operations and structure, as well as current and proposed privacy initiatives for the Department. The letter was formally adopted during the meeting. Since the submission of the letter, the Chief Privacy Officer has referred to the DPIAC's recommendations as she developed her 2009 goals for the DHS Privacy Office and systematizing privacy throughout the Department in the coming year.

On February 26, 2009, the DPIAC held a public meeting in Washington, DC. Following the Acting Chief Privacy Officer's update regarding general DHS Privacy Office activities, the DPIAC heard in-depth presentations by DHS Privacy Office staff on DHS FOIA implementation and recent international outreach activities conducted by the DHS Privacy Office IPP Group. Consistent with the DPIAC's ongoing interest in DHS redress programs, the Director of the TSA Office of Transportation Security Redress provided a comprehensive review of the DHS TRIP program. On May 14, 2009, the DPIAC held another public meeting in Washington, DC, during which the Chief Privacy Officer provided a general update regarding Office activities and detailed her vision for the DPIAC. The Chief Privacy Officer announced that the DPIAC's focus this year would be the Department's engagement with the public. In particular, the DPIAC will focus its advice on matters related to DHS redress programs, individual access to PII, and public education. In keeping with that focus, the US-VISIT Privacy Officer gave a presentation on the US-VISIT program's redress process. Staff of the DHS E-Verify Program provided an update regarding how they addressed the Committee's E-Verify Report recommendations.

The May 14, 2009 DPIAC meeting concluded with Committee deliberations on a draft report setting out guidance for the implementation of DHS Information Sharing and Access Agreements (ISAAs) with external organizations. The DPIAC adopted the report, entitled *White Paper: DHS Information Sharing and Access Agreements* (Report No. 2009-01),[34] which includes recommendations based on the FIPPs framework set out in the DHS Privacy Office's December 2008 Privacy Policy Guidance Memorandum.[35] The report includes recommendations on DHS oversight of ISAAs and conducting an Information Sharing Threshold Analysis for each ISAA. It also provides guidance on ISAA preparation and review, communications supporting ISAAs, and audit procedures related to the information sharing process and ISAA terms. The DHS Privacy Office will use the DPIAC's white paper to inform its efforts to develop information sharing guidance for the Department. The report has been shared with the Secretary of Homeland Security and the Department's ISGB.

Plans are underway for quarterly public DPIAC meetings in the remainder of FY 2009 and FY 2010. The DHS Privacy Office looks forward to working with various DHS programs to evaluate and address recommendations found in the DPIAC's reports in the months ahead.

[34] http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_issa_final_recs_may2009.pdf.
[35] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

IV. Training & Education

The DHS Privacy Office partners with other offices in the Department to develop mandatory privacy training for all employees and contractors and include privacy themes in supplemental training classes. The Office reports quarterly to Congress on its training activities as required by section 803 of the 9/11 Commission Act. The Office also supports targeted training efforts, such as compliance training and specific role-based courses within the Department. These training courses are discussed in the subsections that follow. The DHS Privacy Office also supports privacy training for state and local fusion centers as discussed in Section IX.

A. DHS-wide Internal Education and Training

The DHS Privacy Office continued to execute its ongoing responsibility to ensure that DHS employees understand the privacy implications of their daily work and handle PII responsibly and in accordance with the Privacy Act and DHS Privacy Office guidance. To that end, the Office provided both mandatory and supplemental privacy training for DHS employees in a number of different formats and venues.

1. Mandatory Training

The Privacy Act and OMB Circular A-130 mandate annual Privacy Act training for DHS employees and contractors. The DHS Privacy Office provides introductory privacy training as part of the Department's bi-weekly orientation session for all new employees. This initial privacy training is supplemented by the DHS Privacy Office's *Culture of Privacy Awareness* course, which covers the essentials of the Privacy Act and the E-Government Act, as well as the responsibility of DHS employees to use PII only for authorized purposes and to protect it from misuse or loss. *Culture of Privacy Awareness* is mandatory for all DHS employees and is available to DHS Headquarters employees through DHScovery, the Department's web-based learning management system. The DHS Privacy Office shares the training it develops with components to enable them to leverage the materials and integrate privacy training into their own programs. Several DHS components implemented the *Culture of Privacy Awareness* course through their own learning management systems or worked with the DHS Privacy Office to incorporate it into their own privacy training courses. For example, S&T built a privacy training program using *Culture of Privacy Awareness* as a foundation. Component Privacy Officers also developed component-specific privacy training this reporting year, detailed in Section IX of this report. The Chief Privacy Officer plans on systematizing privacy training across the Department during the next reporting year.

2. Supplement al Training

During the past year, the DHS Privacy Office provided a privacy presentation as part of the two-day *DHS 101* training course, which is offered quarterly to DHS employees seeking an overview of all DHS components' roles and activities. The Office also presented at the OIA's Cross-

Training Session, held for DHS staff who actively engage with other countries and international organizations to support the DHS mission. The DHS Privacy Office explained the role of the Office in the international arena and discussed current international privacy issues.

3. Privacy in Security Training

In August 2008, the DHS Privacy Office participated in the DHS Annual Security Conference sponsored by the CISO. This conference brought together over 3,000 information technology and security professionals throughout DHS. During the event, the DHS Privacy Office conducted sessions on privacy sensitive systems (DHS Directive 4300A Attachment S), privacy incident handling for DHS security personnel, privacy documentation (i.e., Privacy Threshold Analyses (PTAs), PIAs, and SORNs), safeguarding PII, and privacy incident handling.

The DHS Privacy Office also developed privacy training directed toward DHS security managers. The training course addresses ways systems may affect privacy and explains the privacy documentation required to use them. This training is available by request, and has been provided to several DHS components and their security staff.

4. Compliance Training

The DHS Privacy Office conducts quarterly PIA training for all DHS employees and contractors responsible for drafting compliance documents within the components. This hands-on course explains the PIA development and review process, including PTAs, and offers an interactive forum to discuss issues that arise during preparation of PIAs. In June 2009, the DHS Privacy Office hosted its annual compliance training for PTAs, PIAs, and SORNs. The training included a brief history of U.S. privacy laws and a full day discussion about privacy compliance. The training was well attended by both DHS and other federal employees.

B. Role-Based Internal Education and Training

1. DHS Privacy Office Staff Training

In addition to training others, DHS Privacy Office staff participated in national conferences and specialized training programs throughout the year to stay current on recent developments in privacy law and policy. DHS Privacy Office staff regularly attended conferences of the American Society of Access Professionals (ASAP), the professional organization for federal government employees and private citizens working in the field of access to information under the FOIA and the Privacy Act.

2. US-CERT Privacy Training

The DHS Privacy Office conducted its second annual privacy training for U.S. Computer Emergency Readiness Team (US-CERT) personnel on May 27, 2009 and June 4, 2009. The training provided an overview of the legal authorities that define DHS's privacy responsibilities, the FIPPs, DHS privacy compliance procedures, and how all three provide the context and standards for those specific privacy requirements and practices relevant to US-CERT.

3. Intelligence and Analysis Training

All DHS intelligence professionals assigned to state or local fusion centers receive extensive privacy training. Section 511 of the 9/11 Commission Act requires that DHS I&A employees

assigned to state and local fusion centers undergo appropriate privacy training developed, supported, or sponsored by the DHS Privacy Office. As DHS employees, intelligence professionals selected for deployment to state and local fusion centers are required to take the DHS-wide *Culture of Privacy Awareness* course. As soon as these intelligence professionals are identified to the DHS Privacy Office, they are provided a CD-ROM of the course. The intelligence professionals are expected to complete this training program before the next stage of their privacy training, the classroom instruction led by a DHS Privacy Office member entitled *Privacy Fundamentals for Intelligence Professionals*.

The first half of the *Privacy Fundamentals* course provides an overview of the Privacy Act and E-Government Act, a discussion of the FIPPs, and an explanation of privacy rules for sharing information, with particular emphasis on the I&A system of records and published routine uses. The second session covers rules for safeguarding PII, employee responsibilities to recognize and address privacy incidents, and privacy considerations when drafting products for wide dissemination. Students are encouraged to ask questions relevant to their individual fusion center's procedures. The DHS Privacy Office has delivered the Privacy Fundamentals course to DHS employees assigned to fusion centers during the past year and will offer the course whenever new employees are selected.

C. DHS Speaker Series

The DHS Privacy Office is in its second year of hosting the DHS Privacy Office Speaker Series. The Speaker Series provides the Office an opportunity to host outside experts for informal discussions with DHS staff on privacy-related topics. The DHS Privacy Office hosted four experts who discussed the follow topics during the reporting period.

1. Privacy Protection Challenges Posed by the Information Sharing Environment

The Center for Democracy & Technology's (CDT) Vice President for Public Policy opened this year's Speaker Series in September 2008. The discussion centered on the unique challenges posed by the ISE for privacy protection policies and procedures. Participation in the event helped inform the DHS Privacy Office's work internally with the ISGB and ISCC and externally with other Departments and Agencies through the ISE.

2. Histori c Trends in Privacy and Security

Later in September 2008, the Chair of the American Bar Association (ABA) Committee on Government Information & Privacy (and University of Cincinnati College of Law professor) spoke with DHS about the historic trends in privacy and security within the U.S. and Europe. The speaker shared insights regarding the historic tradeoffs between privacy and security and discussed how they may be reconsidered in the future. The speaker provided helpful background and context for the DHS Privacy Office's continued work on international privacy issues, as well as the Office's collaboration with CISO and the DHS Office of Cybersecurity and Communications (CS&C).

3. Historical Regulation of Website Technologies

In April 2009, the DHS Privacy Office hosted CDT's Vice President and Chief Operating Officer who discussed the government's historical regulation of website technologies and the specific challenges that new tracking technologies pose for privacy in the modern digital era. This speaker later participated in the DHS Privacy Office's Government 2.0 Workshop and built upon the informal discussion he began with DHS and Office staff in April.

4. Trends in Cyber Crime and Cybersecurity Strategies

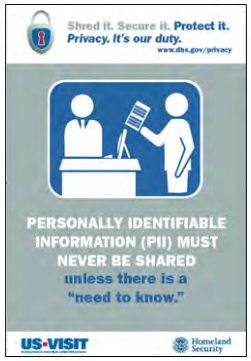
In May 2009, the SANS Institute's Director of Research spoke with DHS about the characteristics and tactics of cyber crime, government trends in cybersecurity, and new strategies for improving cybersecurity. He engaged DHS staff in a lively discussion regarding general security issues and specific challenges facing government. This discussion generated much interest within DHS and was a precursor to the cybersecurity panel included in the Government 2.0 Workshop.

D. Component Privacy Weeks

The DHS Privacy Office fosters a culture of privacy throughout the Department, and encourages components to reinforce this culture through initiatives within their component. Several components began hosting annual privacy events in FY 2009. The events, which met with much success, are described in following sections.

1. US-VISIT

In October 2008, US-VISIT held its first annual Privacy Awareness Week. The event provided an opportunity for every US-VISIT employee and contractor involved in the program to recommit to protecting the privacy of individuals whose information US-VISIT maintains. As part of US-VISIT's Privacy Awareness Week, guest speakers spoke to participants about a variety of privacy and security topics including how to foster a culture of privacy and employee responsibilities to protect privacy. US-VISIT is currently planning events for this year's Privacy Awareness Week,



scheduled to take place in October 2009. Posters developed for Privacy Awareness Week remain posted throughout the US-VISIT workplace to serve as a reminder of these important messages.

2. U.S. Citizenship and Immigration Services and E-Verify

In conjunction with the USCIS Privacy Office, the Privacy Branch of the Verification Division successfully organized its first annual Privacy Awareness Month in February 2009 to raise awareness about privacy issues, challenges, rules, and regulations among Verification Division personnel. Activities included a campaign of posters, weekly trivia, games and prizes, and presentations and training sessions on a wide range of privacy-related topics. The program was built around the theme of "Privacy: Like it, Love it, Gotta have it!" and began with an announcement email from the Verification Division Chief describing the Privacy Branch's mission, policy, and principles. Speakers throughout the month included the USCIS Privacy Officer and Deputy Privacy Officer; Executive Director, Office of Privacy & Disclosure, Office of the General Counsel, SSA; and members of the DHS Privacy Office. The program focused on raising awareness of privacy issues among all division employees, as well as incorporating privacy into projects and everyday duties of managers and team leaders.

3. Science and Technology

On May 11-15, 2009, S&T held its second annual privacy awareness training event. S&T extended this year's event from Privacy Day to Privacy Week to include additional training activities and allow for more flexibility in individual schedules. During Privacy Week, S&T accomplished the following objectives:

- Conducted Directorate-wide mandatory annual privacy awareness training for over 600 S&T employees and contractors;
- Provided supplemental training for Program Managers and Division Directors that focused specifically on the *Principles for Implementing Privacy Protections in Research Projects* (S&T Research Principles) developed jointly by S&T and the DHS Privacy Office; [36]
- Audited mobile devices to ensure compliance with DHS policies and regulations regarding the storage and retention of PII;
- Conducted a "file clean up" where S&T personnel reviewed paper and electronic files to identify PII, delete or dispose of files that are no longer needed, and protect files that must be retained properly;
- Sent out daily emails with privacy tips/reminders to all S&T employees and contractors to promote Directorate-wide awareness of responsibilities in protecting and safeguarding privacy;
- Coordinated a Q&A session with the DHS Privacy Office in which several S&T Program Managers met with the DHS Privacy Office to discuss privacy concerns and questions related to specific projects; and
- Coordinated with CRCL to provide an informational training session for S&T Program Managers and Division Directors to help them identify projects that may have civil liberties implications.

[36] The S&T Research Principles are discussed in Section X.A and included in Appendix C of this report.

Overall, S&T Privacy Week was a great success and demonstrated S&T's continuing commitment to privacy.

4. U.S. Coast Guard

The USCG Privacy Office conducted its second Annual Privacy Awareness Week June 22-26, 2009. USCG Privacy Office personnel hosted a table in the Coast Guard Headquarters cafeteria, accessible to several thousand military and civilian employees and contractors, providing educational and informational material:

- Guidebooks and templates needed to complete privacy compliance documentation (i.e. PTAs, PIAs, and SORNs);
- *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*;
- Posters reminding personnel of the importance of daily adherence to privacy procedures; and
- USCG reporting requirements when either a suspected or confirmed incident involving the loss or compromise of PII occurs.

Privacy Staff engaged with personnel, answered questions, and distributed a list of basic "Do's and Don'ts" to increase privacy awareness. Further, the USCG Privacy Office coordinated with the DHS Privacy Office to conduct PTA and PIA training for Program Managers. The DHS Privacy Office provided a comprehensive step-by-step presentation of the requirements and processes for writing and submitting each of these privacy compliance documents.

E. Certification

During this year, the DHS Privacy Office continued to develop the expertise of its privacy/FOIA professionals by encouraging participation in certification programs and training courses to enhance their skills and abilities while furthering the mission of the Office and Department. Several DHS Privacy Office staff members were successful in obtaining the International Association of Privacy Professionals (IAPP)[37] Certified Information Privacy Professional/Government (CIPP/G) certification. This certification is the first publicly-available privacy certification designed for federal government employees with privacy-related responsibilities or obligations, such as privacy officers, compliance managers, records managers, access-to-information coordinators, information security managers, and information auditors. To be recognized as a CIPP/G, privacy professionals must pass both the IAPP's Certification Foundation and CIPP/G examinations. At the conclusion of reporting year, 16 staff in the DHS Privacy Office held the CIPP/G certification. Additionally, 10 staff held the CIPP/G certification in other components, directorates, and program privacy offices. The DHS Privacy Office encourages privacy staff throughout DHS to obtain this certification.

[37] www.privacyassociation.org.

V. Policy Initiatives

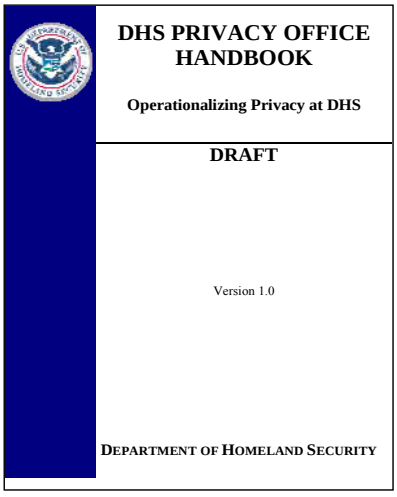
A. Information Sharing

As previously noted, IRTPA established the ISE to share terrorism-related information in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties. In support of this requirement, the Program Manager for the ISE (PM-ISE) issued ISE *Guidelines to Ensure that Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*[38] (ISE Privacy Guidelines) in December 2006. The ISE Privacy Guidelines require relevant entities to implement a written privacy protection policy that is at least as comprehensive as these guidelines.

The *DHS Privacy Office 2008 Annual Report* noted that the DHS Privacy Office would turn its attention to identifying, assessing, and documenting the Department's ISE-compliant privacy policy. Implementing that promise and consistent with the Department's commitment to protecting privacy as a participant in the federal ISE, the DHS Privacy Office disseminated the *DHS ISE and Civil Liberties Protection Policy*[39] to DHS employees and made it available to the public through its website. The policy outlines how the Department protects privacy, civil rights, and civil liberties when sharing covered information within the ISE.

This policy was developed jointly by the DHS Privacy Office and CRCL, and is representative of the close working relationship that exists between the two offices. As noted in the June 2009 *ISE Annual Report to Congress*, DHS is currently one of only a few federal agencies to have such a policy in place.[40] DHS is also the first federal agency to make its policy available to the public.

B. Privacy Handbook


DHS PRIVACY OFFICE HANDBOOK

Operationalizing Privacy at DHS

DRAFT

Version 1.0

DEPARTMENT OF HOMELAND SECURITY

During FY 2009, the DHS Privacy Office developed the *DHS Privacy Office Handbook* (Privacy Handbook), a single resource for in-depth information regarding DHS Privacy Office functions. It describes how the DHS Privacy Office "operationalizes" privacy.

The purpose of the Privacy Handbook is to inform the Department, other federal agencies, and the public about the DHS Privacy Office and provide transparency into its various functions and operations. The Privacy Handbook will also aid in orienting new DHS Privacy Office personnel, new component Privacy Officers and PPOCs, other federal privacy

[38] http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.
[39] http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.
[40] The PM-ISE's Annual Report may be found at http://www.ise.gov/docs/reports/ISE_2009-Annual-Report_FINAL_2009-06-30.pdf.

officers, and even international privacy offices by providing insight into how DHS builds its privacy culture.

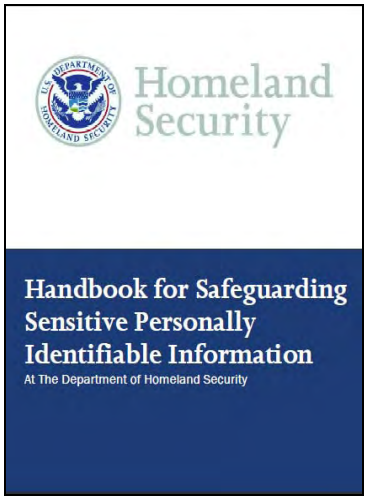
The Privacy Handbook discusses the DHS Privacy Office's role and responsibilities as stewards for privacy within the Department. It covers such areas as policy, compliance, education and awareness, complaints and incidents, public outreach and transparency, international activities, disclosures and FOIA operations, and reporting. The Privacy Handbook summarizes, but does not replace, existing DHS Privacy Office policies, procedures, and guidance. It is expected to be released in September 2009.

C. FIPPs Framework

In December 2008, the DHS Privacy Office issued a guidance memorandum memorializing the FIPPs as the foundational principles for privacy policy and implementation at DHS[41] – *Privacy Policy Guidance Memorandum 2008-01*, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*.[42] The Chief Privacy Officer's authority to establish these principles as the framework for privacy policy at DHS is based upon sections 222 (a)(1) and (a)(2) of the Homeland Security Act as amended,[43] which authorize the Chief Privacy Officer to assume primary responsibility for DHS privacy policy, including (1) assuring that the use of technologies sustains and does not erode privacy protections relating to the use, collection, and disclosure of personal information; and (2) assuring that personal information contained in DHS Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act.

The FIPPs have served as the basis for numerous policy and compliance activities within the DHS Privacy Office during this reporting period, including PIAs, the CCTV workshop report on best practices for the use of CCTV, the State and Local Fusion Centers PIA, and the privacy principles for S&T research referenced in the 2008 Data Mining Report. The DHS Privacy Office continues to find this framework essential in ensuring that privacy considerations are addressed whenever these principles are applied to activities within DHS or internationally.

D. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS



In October 2008, the DHS Privacy Office issued its *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS,*[44] which sets policy on how DHS employees and contractors must safeguard sensitive PII. This is intended to help DHS personnel safeguard sensitive PII in paper and electronic form during their everyday work activities to reduce the risk of serious

[41] See Appendix A and the DHS Privacy Office's *2008 Annual Report* for a more detailed discussion of the FIPPs implementation.
[42] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[43] Homeland Security Act of 2002, as amended, 6 U.S.C. § 142.
[44] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf.

data breaches. The handbook outlines minimum standards for handling sensitive PII at DHS by providing step-by-step guidance on how to identify and protect it in various circumstances:

- In the office or at an alternate worksite;
- On a portable device, such as BlackBerry or laptop;
- When sent by email, fax, or other electronic transfer;
- When sent by mail: external, overseas, and inter-office;
- When stored on a shared drive; and
- When on official travel.

The handbook also provides simple instructions on how to encrypt and dispose of sensitive PII. The DHS Privacy Office handbook was drafted in response to the requirements of OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*[45] The handbook will be the basis of future training and additional guidance from the DHS Privacy Office.

E. Data Extracts Working Group

In July 2008, the DHS Privacy Office established a Data Extracts Working Group (Working Group) to respond to OMB requirements outlined in OMB Memorandum 07-16 requiring federal agencies to log and track data extracts of sensitive information from systems in computer-readable formats. The Working Group was charged with establishing uniform practices throughout the DHS for authorizing, tracking, and destroying computer-readable extracts (CREs). The Working Group includes members of several DHS components, including TSA, US-VISIT, FEMA, the DHS Privacy Office, USCIS, ICE, FLETC, and S&T.

The Working Group took a risk-based approach to drafting the requirements for managing CREs and focused on non-routine or ad hoc data extracts and methodologies for reducing the likelihood of losing sensitive PII. The Working Group drafted the DHS Guide to Managing Computer-Readable Extracts (CRE Guide), which provides baseline standards to minimize the risks associated with CREs in an effective manner while limiting the impact to DHS business operations. The CRE Guide is scheduled to be published during the next reporting year and will become effective 90 days following the date of publication.

In addition to drafting the CRE Guide, the Working Group has been researching various technologies and IT providers who may be able to provide technical solutions for managing CREs, as well as addressing other concerns regarding data loss prevention solutions.

[45] http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-16.pdf.

VI. Compliance Activities

The DHS Privacy Office Compliance Group (Compliance Group) is responsible for privacy implementation across DHS. The Compliance Group, which is led by the Director of Compliance, supervises the completion and approval of all PTA, PIAs, and SORNs throughout the Department. In addition, the Compliance Group is responsible for meeting statutory requirements such as Federal Information Security Management Act of 2002 (FISMA)[46] privacy reporting, 803 reporting, OMB 300 reviews, Enterprise Architecture Board (EAB) reviews, compliance reviews, as well as outreach to the component Privacy Officers and PPOCs to ensure privacy compliance requirements are met. The process for handling these responsibilities, including the compliance documentation, has matured since the inception of the DHS Privacy Office and will continue to do so in the future.

The major accomplishments for the Compliance Group during this reporting period were (1) continuing to build and strengthen the overall privacy compliance process, (2) instituting a formal process to review PTAs on a rolling three-year basis, (3) issuing the *Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments*,[47] (4) re-issuing the legacy agency SORNs under the Department's authorities, and (5) continuing to build the network and relationships with component Privacy Officers and PPOCs.

As the compliance program continues to mature, the focus will expand from merely reviewing new programs and IT systems to conducting in-depth periodic reviews of existing programs to ensure they continue to meet the standards set forth in published privacy compliance documentation.

A. Overview of the Privacy Compliance Process

DHS has three main documents related to privacy compliance: (1) the PTA, (2) the PIA, and (3) the SORN. Each of these documents plays a distinct role in the Department's privacy activities.

1. PTAs

The PTA is the first document completed by a program seeking to implement a system, program, or project. The PTA identifies whether the system is a Privacy Sensitive System (i.e., a system used to collect and maintain PII). The PTA also identifies whether additional privacy compliance documentation such as a PIA or SORN is required.

2. PIAs

PIAs are an important tool for examining the privacy impact of IT systems, programs, or projects. The PIA is the method by which the Compliance Group reviews system management activities in key areas such as security and how/when information is collected, used, and shared.

[46] Title III, E-Government Act of 2002, Pub. Law 107-347, 116 Stat 2899, 2946 (Dec.17, 2002).
[47] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.

If a PIA is required, the program will draft the PIA for review by the component Privacy Officer/PPOC and component counsel. Part of the PIA analysis includes determining whether an existing SORN appropriately covers the activity or a new SORN is required. Once the PIA is approved at the component level, the component Privacy Officer or PPOC submits it to the DHS Privacy Office Compliance Group for review and approval.

3. SORNs

SORNs provide notice to the public regarding Privacy Act information collected by a system of records, as well as insight into how information is used, retained, and may be corrected. Part of the Privacy Act analysis requires determining whether certain Privacy Act exemptions should be taken to protect the records from disclosure to an individual because of law enforcement and/or national security reasons. If a SORN is required, the program manager will work with the component Privacy Officer or PPOC and component counsel to write a SORN for submission the DHS Privacy Office.

While the requirements for these documents stem from different sources, they often work in tandem to identify and document areas of privacy focus for programs, IT systems, and collections of records. Examples of how these documents may work together appear in **Figure 3.**

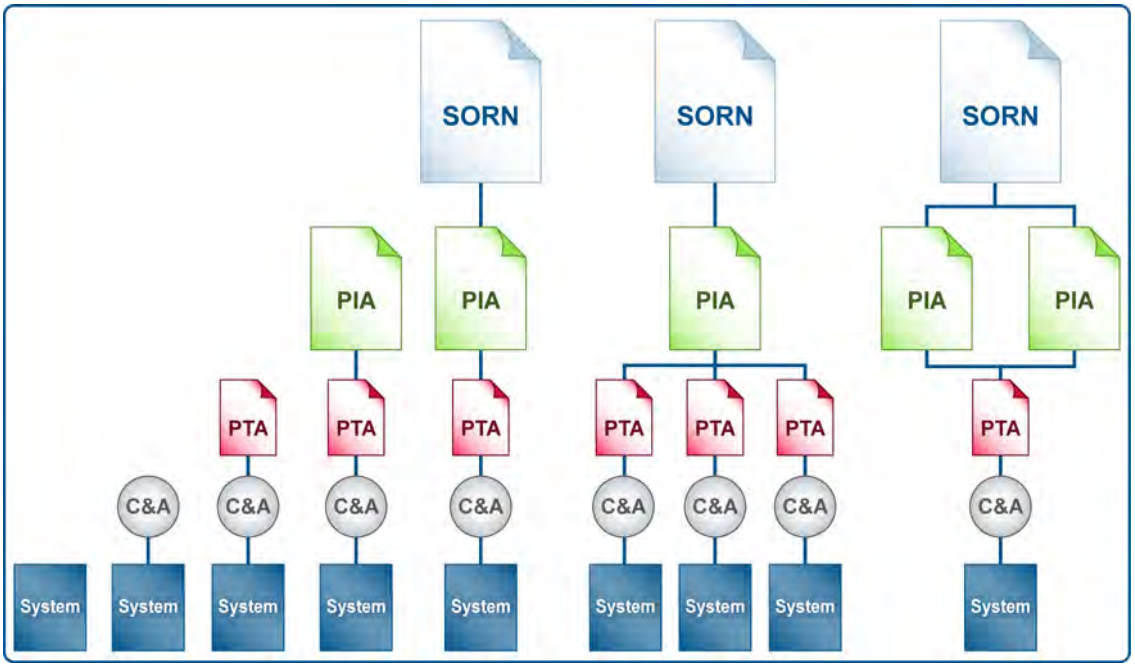


Figure 3: DHS Privacy Document Process Examples

Once the PTA, PIA, and SORN are completed, the documents are periodically scheduled for a mandatory review by the DHS Privacy Office (timing varies by document type). For systems that require only PTAs and PIAs, the process begins again three years after the document is complete or when there is an update to the program, whichever comes first. The process begins with either the update or submission of a new PTA. The Privacy Act requires that SORNs be reviewed on a biennial basis. The DHS Privacy Office privacy compliance process depicted in

Figure 4 illustrates the iterative process for completing and reviewing compliance documentation.

This circular process enables the DHS Privacy Office to regularly review both new and existing programs to ensure they continue to comply with privacy laws and regulations. Section VI.B below describes each of these activities in greater detail.

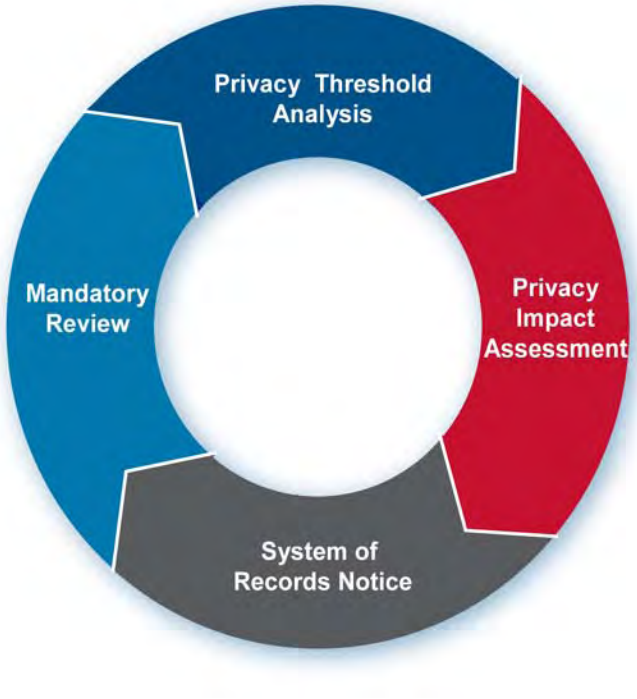


Figure 4: DHS Privacy Office Privacy Compliance Process

B. Strengthening the Privacy Compliance Process

1. PTAs

In November 2005, the DHS Privacy Office developed and incorporated the PTA into the Certification and Accreditation (C&A) process as a means of systematically assessing the privacy protectiveness of information technology (IT) systems. The PTA became mandatory in January 2006 for all IT systems with a requirement that it be updated no less than every three years to coincide with the C&A process.

Over the last three years, the PTA has developed into the mechanism by which the DHS Privacy Office formally documents decisions for IT systems going through C&A, and those made by programs, affecting privacy. For example, PTAs are now used to document and track all systems collecting Social Security Numbers (SSNs) from the public. The DHS Privacy Office also developed specific PTAs for certain DHS-wide types of data collections, such as contact lists. Programs that maintain contact lists complete the Contact List PTA to attest that their program meets the requirements laid out in the DHS-wide Contact List PIA. This has reduced the number of individual PIAs that programs are required to complete while ensuring DHS programs use PII consistently for contact lists.

The PTA documents whether the system maintains PII, as well as whether a PIA and/or a SORN is required. If the PTA identifies an IT system that has PII, the security requirements are tailored to that determination.

In January 2009, the DHS Privacy Office began conducting a review of PTAs more than three years old. The PTA template is frequently updated to improve its content and address new processes. By reviewing systems against the new PTA, the DHS Privacy Office obtains increased assurance that it is identifying those systems that are privacy sensitive. PTAs will

continue to be reviewed on a rolling three-year basis. From July 1, 2008, through June 30, 2009, the DHS Privacy Office reviewed and validated 430 PTAs.[48]

2. PIAs

The PIA is a crucial mechanism used by the Chief Privacy Officer to fulfill statutory mandates and to operationalize privacy across DHS. The PIA is considered a deliberative document and requires a program to consider privacy throughout its development lifecycle.[49] The PIA provides the public greater transparency of government operations, often more so than the SORN. The E-Government Act and Homeland Security Act require completion of PIAs, and in some cases Congress has tied program funding to completion of a PIA.

The DHS Privacy Office coordinates the completion of PIAs for DHS 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.[50] Between July 1, 2008 and June, 30, 2009, the DHS Privacy Office approved and published 61 PIAs. The DHS Privacy Office also reviewed and approved several PIAs for National Security Systems for I&A. Those PIAs were conducted to integrate privacy protections into I&A programs and provide assistance and oversight to Congress, the Office of Inspector General (OIG), and the DHS Privacy Office prior to deployment. Due to the sensitivity of data in the systems, PIAs for national security systems are not published. **Figure 5** illustrates the number of public PIAs completed by each component during this reporting year. Appendix B provides a complete list of approved and published PIAs.

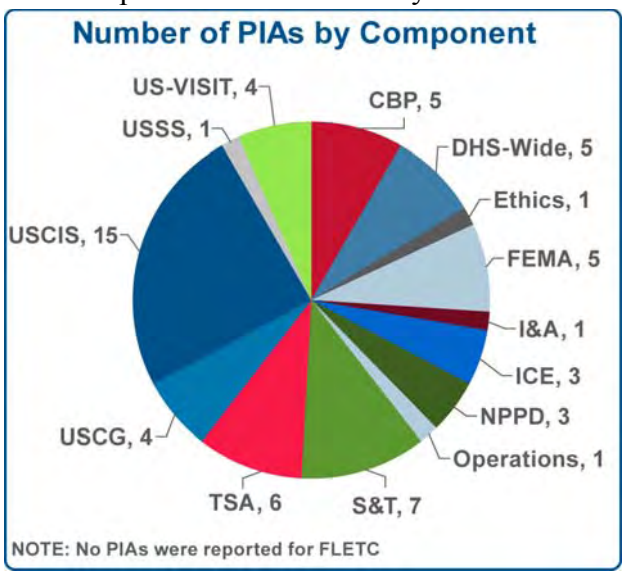


Figure 5: Number of PIAs Completed by Component during the Reporting Year

a. Privacy Policy Guidance on Privacy Impact Assessments

The FIPPs guidance issued in December 2008[51] provides an articulated standard by which the DHS Privacy Office can assess the impact on privacy. Using the FIPPs as a tool when developing PIAs has strengthened the analytical process associated with the PIAs. DHS has developed two distinct templates for PIAs – the more IT-centric PIA and the FIPPs-based PIA. DHS Privacy Office works with programs to determine which PIA best fits their program.

[48] Totals include new PTAs, as well as PTAs included in the three year review cycle.
[49] The term "development lifecycle" refers to the phases of program or system development from conception, design, development, testing, and deployment, to retirement.
[50] PIAs are posted at the following link on the DHS Privacy Office website: www.dhs.gov/privacy, then follow links to Privacy Impact Assessments.
[51] See Section V.C and Appendix A for more information about the FIPPs.

The Office has also issued its *Privacy Impact Assessment Official Guidance*[52] designed to discuss the various statutory requirements of the E-Government Act at DHS and to guide the process of drafting a PIA. This PIA guidance and an associated PIA template are used by the components and Headquarters staff responsible for drafting PIAs for their programs and systems. Originally published in 2005 and revised in 2007, the Department's PIA Guidance has been used as a model by other federal agencies. The PIA touches on general areas such as scope of information collected, use of information collected, information security, and information sharing. The PIA also presents specific questions regarding the use of commercial data, data analysis tools, and compliance with the relevant system's SORN. Furthermore, each section of the PIA concludes with an analysis section designed to outline any privacy risks identified in the preceding section's questions and to discuss any strategies or practices used to mitigate those risks. The analysis sections reinforce critical thinking about ways to enhance the natural course of system development by including privacy in early stages.

The DHS Privacy Office also formalized its policy specifying when a PIA is required at the Department in its *Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments*.[53] This policy does not lay out new requirements; rather, it formalizes the circumstances under which DHS conducts a PIA. PIAs are required when developing or issuing any of the following:

- **IT systems** that involve PII of members of the public, as required by section 208 of the E-Government Act of 2002;
- **Proposed rulemakings** that affect PII, as required by section 222(a)(4) of the Homeland Security Act;
- **Human resource IT systems** that affect multiple DHS components, at the direction of the Chief Privacy Officer;
- **National security systems** that affect PII, at the direction of the Chief Privacy Officer;
- **Program PIAs**, where a program or activity raises privacy concerns;
- **Privacy-sensitive technology** PIAs, based on the size and nature of the population impacted, the nature of the technology, and the use of the technology is high profile; and
- **Pilot testing** when testing involves the collection or use of PII.

Figure 6 depicts the percentage of DHS PIAs published in FY 2009 by type.

[52] http://www.dhs.gov/files/publications/gc_1209396374339.shtm.
[53] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.

A list of all PIAs published during the reporting period is provided in Appendix B. A few examples are discussed below.

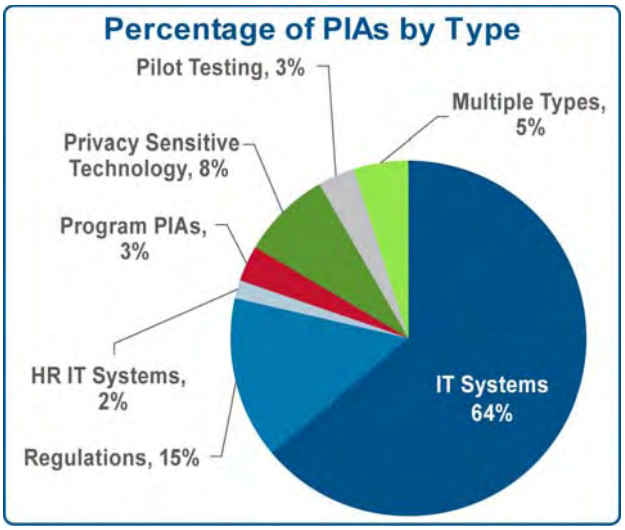


Figure 6: PIAs Published by DHS during the Reporting Year

USCIS Case Management System

DHS published the PIA, SORN, and Privacy Act exemptions for the USCIS Fraud Detection and National Security System Data System (FDNS-DS). FDNS-DS is a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety, and national security concerns. The FDNS-DS system is an upgrade of the Fraud Tracking System (FTS). The FTS PIA was first published on June 24, 2005. The PIA identified the risk of using public source information to identify possible fraud. There is a risk that inaccurate or incorrect information will be used to make a determination. To mitigate this risk, FDNS officers may only use the public source information to verify information already on file to identify possible inconsistencies. If the information is derogatory, pertinent to adjudication, and will be used in the adjudication process, the USCIS must by law notify the individual and provide him or her with an opportunity to respond.

USCG Notice of Arrival Rulemaking

DHS issued a number of regulations during the reporting period that impacted PII. Under section 222(a)(4) of the Privacy Act, the DHS Privacy Office issued a PIA for USCG's Notice of Arrival and Departure rulemaking. The rule proposed to expand the applicability of notice of arrival (NOA) requirements to additional vessels, establish a separate requirement for certain vessels to submit notices of departure (NOD), set forth a mandatory method for electronic submission of NOA and NOD, and modify related reporting content, timeframes, and procedures. The privacy implication of collecting additional information from different types of vessels was identified and addressed in the PIA process. USCG issued a new SORN to cover the collection of certain passenger and crew information.

Closed-Circuit Television (CCTV)

The DHS Privacy Office has developed a CCTV PIA template that asks targeted questions associated with the development and deployment of CCTV technologies. This PIA, which was first used in July 2007 with the Secure Border Initiative (SBInet), was used with an S&T research project titled "Reality Mobile Kentucky Project" during this reporting period. The Reality Mobile Kentucky Project is an S&T research and development effort that seeks to test the operational effectiveness and efficiency of streaming video for law enforcement applications. S&T conducted the PIA because the project requires the Kentucky State Police to capture images of individuals during the field test in accordance with their law enforcement authorities, standard operating procedures, and applicable state and local laws.

Implications of Fusion Centers

The DHS Privacy Office used the FIPPs PIA template to discuss the implications of the DHS State, Local, and Regional Fusion Center Initiative (Fusion Center Initiative) on privacy. Under the Fusion Center Initiative, DHS will facilitate appropriate, bi-directional information sharing between DHS and state, local, and regional fusion centers. The PIA identified a number of areas where DHS has developed appropriate privacy mechanisms for handling the risks associated with the program, which included: (1) justification for fusion centers; (2) ambiguous lines of authority, rules, and oversight; (3) participation of the military and the private sector; (4) data mining; (5) excessive secrecy; (6) inaccurate or incomplete information; and (7) mission creep.

3. SORNs

As discussed previously, 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 disposition, and retrieval process of the system. It also describes any applicable Privacy Act exemptions.

a. Legacy SORN Update Project

In FY 2009, DHS completed its review and update of legacy agency SORNs (i.e., SORNs carried over from legacy agencies when DHS was created in January 2003). While a savings provision within the Homeland Security Act preserves the coverage of these legacy SORNs, the Chief Privacy Officer increased resources in September 2007 to enable the DHS Privacy Office to move the review forward in a more coordinated and expeditious fashion. The DHS Privacy Office and components performed the following activities to support this effort:

- Reviewed and identified obsolete and out-of-date SORNs;
- Developed a consistent privacy approach for DHS records;
- Updated SORNs to reflect the mission of the DHS; and
- Increased transparency to the public and DHS employees about the use of PII.

In FY 2009, the DHS Privacy Office conducted an extensive review of 211 legacy SORNs. As a result of this effort, DHS retired 19 obsolete SORNs and published 65 new SORNs. The newly-issued DHS SORNs provide significant notice and transparency of DHS operations and give the public a meaningful opportunity to participate in the rulemaking process. This effort brought the DHS one step closer to the Department's goal of becoming "One DHS" by providing consistent rules for handling PII in SORNs across the Department.

b. SORN Guidance and Templates

As part of the Legacy SORN Update Project, DHS updated the SORN and Privacy Act exemption templates to streamline the process and provide components with tools that were easier to use.

c. Biennial SORN Review

With the retirement of the legacy agency SORNs and publication of new DHS SORNs, the DHS Privacy Office has begun focusing on the required biennial SORN review required under the Privacy Act. SORNs requiring a biennial review were prioritized based on whether they were reviewed as part of the Legacy SORN Update Project. Additionally, the DHS Privacy Office developed a calendar for reviewing all of the Department's SORNs on a biennial basis along with a checklist and guidance to support components in their review of the SORNs. **Figure 7** depicts the number of SORNs published by each component during the reporting year. A complete list of published SORNs is provided in Appendix C.

C. Program Identification and Oversight

The DHS Privacy Office identifies programs that must go through the privacy compliance process through three main avenues: (1) the FISMA C&A process; (2) the OMB 300 budget process; and (3) the Enterprise Architecture Center for Excellence (EACOE) process. Working with the CIO and Chief Financial Officer (CFO), the DHS Privacy Office provides subject matter expertise for reviews of new IT programs and newly budgeted programs to identify privacy compliance issues.

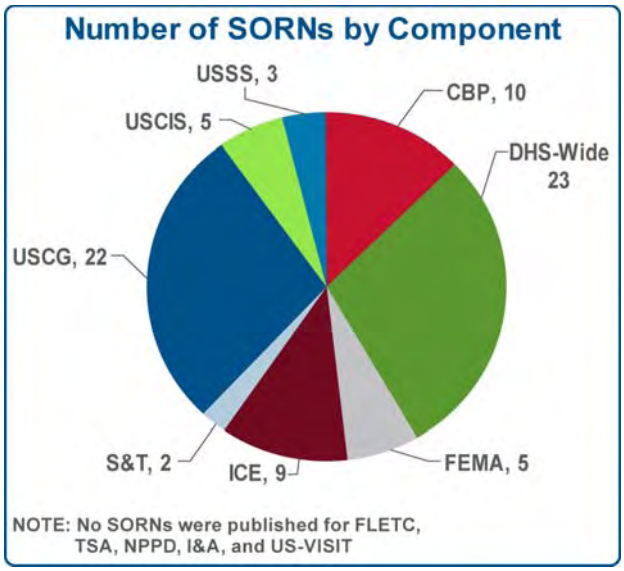


Figure 7: Number of SORNs Published by Component during the Reporting Year

1. FISMA Privacy Reporting

Privacy and information security are closely linked, and strong practices in one area typically support the other. Ensuring security of PII is one of the FIPPs. To that end, the DHS Privacy Office works closely with the CISO to monitor privacy requirements under FISMA. 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 process. At the end of the FY 2008 reporting period, October 1, 2008, DHS had conducted PIAs on 50% of the IT systems that required PIAs. Ninety-one percent of the IT systems were covered by a SORN. By July 1, 2009, DHS had improved its FISMA privacy numbers to 58% for PIAs and 93% for SORNs. The components and/or programs with the best scores were TSA and S&T. The Chief Privacy Officer has met with below average components to discuss ways to ameliorate their performance, and hopes to see improvements in the next reporting year.

2. OMB Exhibit 300s

All major DHS programs are reviewed by the DHS Privacy Office 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 DHS Privacy Office's review is both substantive and procedural, ensuring that each investment has the proper privacy documentation in place at the correct time. Specifically, the review of each 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 Compliance Group then works with each investment program manager to complete necessary documents. The DHS Privacy Office works in close cooperation with the DHS CIO and CFO to ensure that Department's IT investments meet the established legal and policy standards set forth by DHS, OMB, and Congress.

During the FY10 budget review process,[54] the Compliance Group reviewed investments and associated systems. To receive a passing score, submissions had to include the appropriate privacy documentation or have a completed PTA on file if the DHS Privacy Office determined the investment would not require additional privacy documentation. Based on these requirements, the DHS Privacy Office failed nine investments due to insufficient privacy protections and privacy documentation. Failing the OMB 300 resulted in programs being placed on the OMB Management Watch List, which raised the issue to senior DHS management and increased OMB reporting requirements until the issues were resolved.[55] The Compliance Group worked closely with the nine failed programs to ensure the appropriate protections and privacy documentation were in place

During this reporting period, the DHS Privacy Office was able to help two programs resolve privacy issues effecting investments by helping them complete PIAs: the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum PIA;[56] and the USCIS Computer Linked Application Information Management System PIA.[57] Both were published in September 2008, allowing the CLAIMS 3 and CLAIMS 4 investments to be removed from the OMB Management Watch List. Both of these investments were on the OMB Management Watch List for several years prior. At the end of the reporting period, the DHS Privacy Office was in the process of the FY 2011 review.

3. Enterpri se Architecture Board

As a means of ensuring that privacy is considered at the beginning of every IT development effort, the DHS Privacy Office sits on the Enterprise Architecture Board. 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 DHS Privacy Office sits on the EACOE and reviews each request for new technology to ensure that the Department's use of technology sustains privacy protections.

[54] The FY10 budget review process took place between June and August 2008.
[55] The OMB 300 process was modified for FY 2011.
[56] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.
[57] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims4.pdf.

D. Compliance Reviews

As the DHS Privacy Office moves into a review cycle with its privacy compliance documentation, it plans to strengthen the process associated with existing programs and existing documentation. The PNR review is an example of this effort.

1. Passenger Name Record Data

In July 2007, DHS and the Council of the European Union (Council) signed an agreement and exchanged letters regarding the transfer of PNR data to DHS by air carriers operating flights between the U.S. and the EU. The agreement included a provision to "periodically review the implementation of this agreement, the DHS letter, and U.S. and EU PNR policies and practices" to assess the "effective operation and privacy protection of their systems."

On December 18, 2008, the DHS Privacy Office released its report titled *Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union*.[58] In its report, the DHS Privacy Office reviewed efforts by CBP and the DHS Office of Policy to fully implement the provisions of the Agreement and Letters and the representations in the Automated Targeting System (ATS) SORN. The report provided findings in the following areas: continued compliance, follow up on the *2005 Report Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union* (2005 Report),[59] and the 2008 remediation and recommendations. Each finding is further discussed below.

- **Continued Compliance:** The DHS Privacy Office found CBP to be in compliance with the Privacy Act and the representations made in the 2007 agreement. The Office received no reports of misuse of PNR since the previous review in 2005 and found that CBP provided required training for those who access PNR. CBP also took extensive measures to ensure appropriate handling of PNR.
- **Follow Up on the 2005 Report:** The 2005 report required follow up on the retention schedules and the routine review of uses of PNR by CBP's OIA. In response to a 2005 recommendation from the DHS Privacy Office, the CBP OIA established a plan to review audit logs associated with CBP's ATS on the use of PNR information. Since May 30, 2005, the CBP OIT has conducted weekly audits of the system to identify instances of unauthorized use. These weekly audits ensured that the PNR was not accessed by unauthorized users, and was used in a manner consistent with their collection. Furthermore, as stated in the August 2007 PIA for the ATS, the National Archives and Records Administration (NARA) approved the current records schedule for PNR in ATS in spring 2005, mitigating the need for additional follow up on the retention schedule.
- **2008 Remediation and Recommendations:** The remediation and recommendations arising from the 2008 PNR Review focused on notice, access, and updating field guidance. As part of the 2008 review, the DHS Privacy Office found that the public notice for PNR, including

[58] A Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union (Dec. 18, 2008) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.
[59] 2005 Report Concerning Passenger Name Record Information Delivered from Flights between the U.S. and European Union (Sep. 19, 2005) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_rpt_09-2005.pdf.

the Frequently Asked Questions and the PNR Privacy Statement, reflected the 2004 agreement rather than the current 2007 agreement.[60] CBP updated these documents and is working to publish them on their website. The access section focused on compliance with the Privacy Act and the FOIA. The DHS Privacy Office found that Privacy Act/FOIA requests were not handled in a timely or consistent manner and recommended additional staff to handle the large volume of requests. The DHS Privacy Office also suggested CBP provide comprehensive training on FOIA, the Privacy Act, DHS policy, and relevant CBP SORNs and applicable exemptions. CBP is actively increasing staff to reduce the backlog and provide more timely responses, and has released procedures for handling requests and exemptions under the Privacy Act/FOIA. The access recommendations also focused on record retrieval and release. With respect to record retrieval and release recommendations, the DHS Privacy Office recommended that CBP ensure that only the PNR information pertaining to the individual requesting information be released, a suggestion that is consistent with the ATS SORN. CBP implemented this recommendation and ensured that all FOIA personnel were trained on the policies outlined in the ATS SORN. CBP issued field guidance in 2004 and provided an update memorandum highlighting the changes between 2004 and 2007. The DHS Privacy Office recommended in its 2008 report that consolidated field guidance be issued for use of personnel who have or may obtain access to PNR.

[60] The 2004 and 2007 agreements are between the EU and US regarding the processing and transferring of PNR.

VII. Cybersecurity

The DHS Privacy Office is responsible for ensuring that all DHS uses of technology include privacy protections. In addition to its privacy compliance role, the DHS Privacy Office also works closely with components to increase awareness of privacy issues and to build privacy policy into the larger framework of the Department's approach to key areas of its responsibility. The Department's work in the cybersecurity area is one example of the DHS Privacy Office's privacy policy role.

The DHS Privacy Office has continued its close working relationship with NPPD's Office of Cybersecurity and Communications (CS&C). CS&C is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. Within CS&C is the National Cyber Security Division (NCSD), which focuses on the cyberspace portions of the overall communications infrastructure. The NCSD's mission is to cooperate with public, private, and international entities to secure cyberspace and America's cyber assets. It does this by maintaining a national cyberspace response system and implementing a cyber-risk management program for protection of critical infrastructure. Within NCSD is US-CERT, the operational arm of NCSD. US-CERT provides response support and defense against attacks for the Federal Civil Executive Branch (.gov). US-CERT also supports information sharing and collaboration with state and local government, industry, and international partners.

During the last reporting period, DHS issued a PIA for EINSTEIN 2, which was the extension of the original EINSTEIN 1 intrusion detection system that DHS provides for federal executive agencies. EINSTEIN 2 included a more detailed analysis of the computer network traffic reviewed by this program. This year, DHS began the process of deploying EINSTEIN 2 to federal government departments and agencies as part of the Trusted Internet Connection (TIC) consolidation program. The purpose of TIC is to reduce the number of federal connections to the Internet, and EINSTEIN 2 will monitor those connection points for malicious activity and alert US-CERT when further protective actions are needed. The DHS Privacy Office continues to participate in the ongoing roll out of the TIC and EINSTEIN services.

The Chief Privacy Officer and staff have met frequently with the leadership of these organizations to reinforce the importance of integrating privacy into the Department's approach to providing cybersecurity. For example, the DHS Privacy Office regularly attends NCSD's weekly cyber planning meeting to stay abreast of the advances in the Department's operational cybersecurity work. In addition, CS&C recently identified a PPOC who attends the Privacy Office's weekly staff meetings. This level of reciprocal coordination ensures that both components are informed and integrated into each other's strategic and working level concerns.

A. White House Cyberspace Policy Review

In the early days of his Administration, President Obama directed the National Security Council and the Homeland Security Council to review the federal government's approach to cybersecurity. In May 2009, the White House issued the report on this review entitled

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.[61] The report emphasizes the importance of the information and communications infrastructure to our economy, our security, and our way of life. The report recognizes the challenges posed by the current architecture of the global digital infrastructure and the specific threats posed by those who seek to exploit the vulnerabilities of this infrastructure. As described in the report, the challenge facing our nation is to continue to benefit from the enormous capabilities of cyberspace, increase the security of that same ever-evolving environment, and accomplish both in such a way that continues promoting and integrating privacy protections.

The report emphasizes the importance of integrating privacy protections into the federal government's cyberspace strategy, starting with the near term goal of designating a privacy and civil liberties official to the National Security Council. The report further emphasized the importance of privacy protections in a number of areas including: identity management, technological capabilities to protect government networks, the role of the Privacy and Civil Liberties Oversight Board, and the overall value in maintaining an open dialog with the privacy community.

During the review, the White House team met with representatives from the privacy and civil liberties communities. The DHS Privacy Office supported the White House team by providing further visibility into the Department's cybersecurity activities, and assisting in meetings with Federal Government privacy and civil liberties officials, as well as with representatives from the privacy and civil liberties communities. These meetings provided an opportunity for the review team to present the purpose and scope of the review and for the privacy community (internal and external to the government) to raise issues and make suggestions to the review team. Some of these issues were captured in the many written comments and insights the review team received, which are available on the White House website.[62] At the request of the review team, the DHS Privacy Office and CRCL coordinated closely with CS&C to host a separate briefing for members of the privacy and civil liberties communities regarding the EISNTEIN program to provide greater transparency into the federal government's cybersecurity activities. In addition to supporting the Administration's cyberspace review and strategy, these outreach efforts further extended the DHS Privacy Office's ongoing practice of providing transparency into DHS activities.

[61] www.whitehouse.gov/asset.aspx?AssetId=1906.
[62] The list of papers submitted to the White House Review Team is available at http://www.whitehouse.gov/cyberreview/documents.

VIII Social Media

On January 21, 2009, President Obama issued the Transparency and Open Government Memorandum[63] directing federal agencies to harness new technologies (i.e., social networking tools) to engage the public. Social networking tools are an effective means by which the federal government can communicate with the public, but the government use of the tools may raise a myriad of complex legal, security, and privacy issues. The DHS Privacy Office is addressing the privacy issues raised by government use of social media in three primary ways. First, in light of the President's Transparency and Open Government Memorandum and to further educate the Department and other agencies, the DHS Privacy Office held a public workshop on privacy issues raised by federal government use of social media. Second, as discussed in Section III.F of this report, the DHS Privacy Office actively participated on the Federal CIO Council's Web 2.0 Subcommittee of the Privacy Committee and provided recommendations to the Privacy Committee on how to promote government use of social media while protecting privacy. Lastly, to address privacy issues raised by social media initiatives taking place within DHS, the DHS Privacy Office participated in an internal social media working group formed to address these issues and is working to develop privacy policies and procedures to govern the implementation of social media initiatives within DHS.

A. Web 2.0 Workshop

On June 22-23, 2009, the DHS Privacy Office hosted a well-attended public workshop that brought together leading academic, private sector, and public sector experts to discuss privacy issues posed by the government's use of social media. The purpose of the workshop was to help federal agencies engage the public by using social media in a privacy-protective manner, and to explore best practices that agencies can use to implement web 2.0 technologies in the spirit of the President's Transparency and Open Government Memorandum. The workshop showcased social media activities on several federal agency websites where the public can actively engage with government. Panelists discussed issues such as the benefits of using social media to expand transparency and participation in government, the privacy and related legal issues raised by government use of social media, and the manner in which the government can best harness these new technologies while protecting privacy. Workshop panelists agreed that the FIPPs are the appropriate framework to use in building privacy protections into federal policy on the use of social media. The DHS Privacy Office also invited interested parties to submit written comments on these issues. The comments and workshop transcript are posted on the DHS

[63] Transparency and Open Government Memorandum, 74 Fed. Reg. 4,685 (Jan. 21, 2009) available at http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf.

Privacy Office website.[64] The DHS Privacy Office will issue a report on the workshop by the end of FY 2009.

B. Department Efforts to Address Social Media

In an attempt to grasp the scope and breadth of social media initiatives taking place in DHS and the associated legal, policy, privacy, and security issues, a Social Media Roundtable Working Group (SMRWG) was formed by the DHS Office of Policy and Office of Public Affairs (OPA) late last year. The SMRWG included representatives from offices throughout the Department and meets to coordinate DHS social media activities.

The DHS Privacy Office is working to implement a privacy compliance process to ensure that the Department's use of social media complies with the Privacy Act, Homeland Security Act, and E-Government Act.[65] The Office has developed a targeted PTA for DHS social media initiatives and has determined that DHS will complete PIAs for DHS social media initiatives. The DHS Privacy Office is in the process of sending the targeted PTA to DHS components to identify the uses of social media throughout DHS and will work with components to complete the PIAs. Lastly, the DHS Privacy Office is working with OPA, OGC, and others to develop policies to govern the use of social media at DHS. A listing of DHS social media websites can be found at: http://www.dhs.gov/xabout/gc_1238684422624.shtm.

[64] The DHS Privacy Office received comments from The Honorable Bennie G. Thompson, Chairman, Homeland Security Committee, as well as several members of the public. The comments are available at http://www.dhs.gov/xinfoshare/committees/editorial_0699.shtm.

[65] The privacy compliance process will determine whether DHS Components are collecting, using, maintaining, or disseminating personally identifiable information and whether the activity triggers the Privacy Act's SORN requirement, as well as ensuring that the activity complies with PIAs that are under development.

IX. Intelligence and Fusion Centers

During the reporting year, the DHS Privacy Office strengthened its relationship with I&A. For the past several years, DHS Privacy Office staff have bolstered their intelligence credentials. Seven DHS Privacy Office staff members hold the security clearances necessary to work closely with I&A personnel and products, nearly that many have attended the Army Judge Advocate's School week-long course on Intelligence Law, and many have attended annual Intelligence Oversight training delivered by the DHS Intelligence Oversight Officer.

While I&A system managers and offices work closely with the DHS Privacy Office's Compliance Group drafting necessary PIAs and SORNs, in recent months the DHS Privacy Office has become more active in helping ensure privacy standards are preserved within DHS intelligence products. Privacy Office staff now review products prepared by I&A analysts to identify possible privacy-related concerns before they are released. This is particularly important given I&A's critical role in disseminating intelligence information outside the traditional federal intelligence community to our information sharing partners in state and local fusion centers.

In addition to this product review, the DHS Privacy Office has committed to crafting written guidance to intelligence analysts who write products and provide training. Together with colleagues in CRCL, the DHS Privacy Office looks forward to further strengthening its relationship with I&A and establishing additional privacy protections within the intelligence activities of the Department.

A. Fusion Centers Background

Section 511 of the 9/11 Commission Act codified the Department's Fusion Center Initiative and established five privacy requirements for DHS and individual fusion centers:

1. **Initial PIA:** Section 511(d)(1) called for the Privacy Office to conduct a PIA as part of the initial program Concept of Operations.
2. **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 9/11 Commission Act.
3. **Privacy training for I&A intelligence analysts:** Section 511(c)(4)(A)(ii) requires that I&A Intelligence Operations Specialists assigned to fusion centers receive appropriate privacy training in coordination with the Chief Privacy Officer.
4. **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" for all state, local, tribal, and private sector representatives within each fusion center.

5. **Information Sharing Environment:** Section 511(i)(3) places fusion center sharing of terrorism information within the scope of the ISE and its privacy protection framework.

The DHS Privacy Office made substantial progress on all of these requirements during the reporting period.

B. PIA and Reporting

On December 11, 2008, the DHS Privacy Office published its *Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative*.[66] Since the Fusion Center Initiative is not a system as defined by the E-Government Act, the DHS Privacy Office conducted a FIPPs-based PIA focusing on transparency and the program's implementation of the FIPPs. In addition, the PIA discusses potential privacy concerns identified by the DHS Privacy Office, other government reviewers (e.g., GAO and the Congressional Research Service), and reports issued by the advocacy community (e.g., the American Civil Liberties Union and the Electronic Privacy Information Center).

While the main focus of the PIA was the Department's Fusion Center program, the PIA made a number of recommendations that individual fusion centers can implement to enhance privacy within their own operations. These suggestions are as follows:

- Implement the Global Justice Information Sharing Initiative's *Fusion Center Guidelines*,[67] particularly as they relate to privacy:
- Draft written privacy policies that are at least as comprehensive as the PM-ISE's *Privacy Guidelines*;
- Continue to follow the work of the PM-ISE, particularly on the Suspicious Activities Reporting (SAR) Initiative;
- Understand state privacy requirements;
- Conduct a PIA of individual fusion centers;
- Take an expansive view of transparency and engage with your local privacy advocacy community; and
- Use the training DHS provides as the starting point for additional training.

The initial PIA concluded with a confirmation from the DHS Privacy Office of our continuing commitment to work with fusion center participants around the country and a preview of the issues to be examined in the follow-up PIA required by section 511 of the 9/11 Commission Act. The DHS Privacy Office has already begun scoping the follow-up PIA and anticipates that it will be completed during the next reporting year.

[66] The Fusion Center Initiative PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf.
[67] *Fusion Center Guidelines* are available at http://www.it.ojp.gov/documents/fusion_center_executive_summary.pdf.

C. Training State and Local Fusion Center Representatives

As noted above, section 511 of the 9/11 Commission Act requires that state and local fusion centers coordinate with the DHS Privacy Office and CRCL to provide privacy and civil liberties training for all state, local, tribal, and private-sector representatives working in fusion centers. To that end, the DHS Privacy Office has developed the *Privacy Fundamentals for Fusion Center Professionals* training course to educate fusion center employees about (1) how to handle PII responsibly and consistent with the FIPPs and applicable privacy laws and (2) how to recognize and address privacy incidents. Representatives of the DHS Privacy Office introduced the training material in March 2009 during a learning lab portion of the National Fusion Center Conference in Kansas City, Missouri.

During this reporting year, the DHS Privacy Office and CRCL jointly initiated a program to deliver the training in person to fusion centers across the U.S., beginning with the fusion center in Baltimore, Maryland. During the coming year, the Office anticipates providing training to a number of fusion centers across the country.

The DHS Privacy Office and CRCL also collaborated with the Department of Justice Bureau of Justice Assistance and the PM-ISE to launch a web-based toolkit that individual fusion centers can use to enhance privacy within their own processes. The web toolkit is available to fusion centers and to the public at http://www.it.ojp.gov/PrivacyLiberty. See Section III.A for additional details regarding DHS Privacy Office collaboration activities with CRCL.

D. Fusion Centers and the Information Sharing Environment

The DHS Privacy Office continued to contribute to the ISE during the reporting year through its support of the PGC's SLWG and influenced development of Global's *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Global's Baseline Capabilities) document written by the DOJ FACA committee and released in September 2008. As discussed in the *DHS Privacy Office 2008 Annual Report*, fusion centers are accustomed to working with Global on a variety of foundational issues. The DHS Privacy Office's efforts to incorporate its recommendations into Global's Baseline Capabilities document helps ensure that fusion centers will use them to evaluate and improve their operations and procedures, including those addressing privacy. Specifically, Appendix II, Section B of Global's Baseline Capabilities document, establishes five detailed privacy requirements for fusion centers:

1. Designate a Privacy Official with well-defined privacy responsibilities;
2. Establish a process for developing a written Privacy Policy that references other fusion center foundational documents, authorities, and procedures;
3. Craft written Privacy Protection Policy that examines the fusion center's activities and is consistent with the ISE Privacy Guidelines, 28 CFR Part 23 Global *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*;
4. Conduct outreach and training based on the standards established in the Privacy Protection Policy; and
5. Ensure accountability within, and to, the standards established in the Privacy Protection Policy; identify methods for monitoring and auditing use of information in the fusion center; permit meaningful individual redress.

The Baseline Capabilities document was also highlighted at the 2009 National Fusion Center Conference hosted by the National Fusion Center Coordination Group.[68] At the Conference, the DHS Privacy Office participated in a panel discussion on the privacy requirements of the Fusion Center Baseline Capabilities exercise. During the panel, the DHS Privacy Office representative urged the fusion centers to go beyond the requirements of the baseline capabilities to issue their own PIAs and adopt a broad understanding of transparency – making as much of their founding documentation and procedures available to the public as possible. The DHS Privacy Office also suggested that fusion center staff should meet regularly with their communities and local privacy advocates. The DHS Privacy Office also co-hosted a booth in the exhibitors' hall with CRCL.

The Chief Privacy Officer reinforced these messages in an address before the National Governors' Homeland Security Advisory Council on June 9, 2009, in Washington DC. In her address, the Chief Privacy Officer noted that weak privacy practices in a single fusion center can negatively impact the public's perception of the entire National Fusion Center program. She urged each member of the council to become personally involved in ensuring privacy is addressed within their state's fusion center. The DHS Privacy Office looks forward to continuing its close partnership with the DHS State and Local Program Management Office and to supporting the DHS Fusion Center Initiative during the coming year.

[68] National Fusion Center Coordination Group includes representatives from the following agencies: DHS; DOJ's Bureau of Justice Assistance, Office of Justice Programs; DOJ's Global Justice Information Sharing Initiative; FBI; Office of the Director of National Intelligence: and the PM-ISE.

X. Technology

A. Privacy Protection in DHS Research Projects

In December 2008, the DHS Privacy Office and S&T announced the new S&T Research Principles. A collaborative effort of both the DHS Privacy Office and S&T, the S&T Research Principles provide a privacy-protective framework for conducting critical homeland security research. They will govern privacy-sensitive research performed at S&T laboratories, S&T-sponsored research conducted in cooperation with other federal government entities, and research conducted by external performers under a contract with S&T.

Consistent with privacy implementation generally at DHS, the S&T Research Principles reflect each of the FIPPs. The S&T Research Principles also include a Privacy Assessment Principle, which reinforces the need to assess the privacy impact of research programs and projects. PIAs will be conducted jointly by S&T and the DHS Privacy Office, and will be an integral part of the development and implementation of any S&T research program or project that is privacy-sensitive and/or involves or impacts PII. The S&T Research Principles are provided in Appendix C of this report.

The DHS Privacy Office is currently working with S&T to complete an implementation plan for applying the S&T Research Principles to privacy-sensitive S&T research projects. In addition, the DHS Privacy Office has prepared a draft Directive for review by senior DHS management, which would establish the S&T Research Principles as the privacy framework for all privacy-sensitive research conducted throughout DHS and its components.

B. Western Hemisphere Travel Initiative

The DHS Privacy Office played a key role in shaping the Western Hemisphere Travel Initiative (WHTI), which is implemented by DHS and the Department of State (State) and requires individuals previously exempt from presenting a passport (e.g., U.S., Canadian, and Bermudian citizens) to present a valid passport or other approved document that establishes the bearer's identity and citizenship when entering the U.S. from within the Western Hemisphere. Phase One, implemented in January 2007, covered the U.S. air travel environment.[69] Phase Two implementation began on June 1, 2009, and includes U.S. land and sea ports of entry.

In the WHTI final rule published on April 3, 2008, DHS designated a limited set of secure documents as WHTI-compliant, which provides DHS confidence in the security of both the physical document and the process by which it was issued. DHS and State engaged the public in the development of new documents that would satisfy WHTI while meeting the specific needs of the border crossing communities and included technology in these documents to facilitate border crossings for travelers.

[69] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_whti_fr.pdf.

The DHS Privacy Office published a series of SORNs and PIAs related to WHTI that provide transparency into the inner workings of the program to both our stakeholders and the general public. These PIAs and SORNs contribute to the understanding of WHTI and how privacy has been addressed. The DHS Privacy Office issued a PIA on the WHTI final rule on March 24, 2008,[70] 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. CBP maintains all border crossing information in the Border Crossing Information (BCI) system, which resides on the TECS platform.[71] On July 2, 2008, the DHS Privacy Office issued a PIA on CBP Board Crossing Operations,[72] which offers additional transparency into many of the documents developed in response to WHTI, specifically enhanced drivers licenses issued by states and Canadian provinces. CBP established NEDS to provide a single purpose data warehouse to maintain the enhanced drivers license (EDL) databases being obtained from states and Canadian provinces to support the expedited processing of EDLs. The DHS Privacy Office published a SORN for BCI[73] and NEDS[74] on July 25, 2008, to provide additional transparency as well as information regarding access and amendment rights.

During the previous reporting year, the DHS Privacy Office issued a PIA that discussed the privacy concerns posed by radio frequency identification (RFID) technology and how the DHS addressed them.[75] The subsequent PIA and SORNs for BCI and NEDS, released during this reporting period, also addressed vicinity RFID technology[76] that is used in these border cards. Some privacy advocates continue to criticize DHS and State on the choice of this technology. However, this technology meets the operational needs of the land border environment by allowing the travel document to be read automatically as a traveler approaches the CBP inspection booth. RFID-enabled documents are issued with protective sleeves that prevent them from being read surreptitiously. Agencies issuing the cards also provide applicants with information about how best to use and protect these documents. DHS and State continued to meet with individuals and organizations with questions about this technology to explain the reason for the decision and the steps implemented to mitigate the privacy risk associated with using it.

[70] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_whti_landandsea_fr.pdf.
[71] The TECS platform was previously called the Treasury Enforcement Communication System. The name of the platform was changed to TECS when ownership was transferred to CBP.
[72] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_borderops.pdf.
[73] http://edocket.access.gpo.gov/2008/E8-17123.htm.
[74] http://edocket.access.gpo.gov/2008/E8-17126.htm.
[75] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_rfid.pdf.
[76] Vicinity RFID technology, as used by DHS, is a passive technology that conforms to the ISO 18000 6-C specification, with a read range up to 30 feet from the reader; however, for operational purposes, CBP reader antennas are tuned to read at a distance of 10 – 15 feet.

XI. Highlights of Component Privacy Programs and Initiatives

Component privacy programs are a critical part of operational privacy efforts across DHS and are responsible for the day-to-day privacy policy, training, and compliance activities within their respective component. During the past several years, these programs have grown significantly. This section highlights some of the key privacy-related activities performed by CBP, FEMA, ICE, S&T, TSA, USCG, USCIS, USSS, and US-VISIT during the past year.

A. CBP

CBP's unique role at the border provides it with access and a mission to collect large amounts of data concerning the persons and commodities crossing the U.S. border. This information serves a variety of border security, trade compliance, and law enforcement purposes for federal and state governments. In addition to the cross component collaboration activities and drafting multiple PIAs and SORNs, CBP devoted significant resources during the reporting period to provide operational support and transactional privacy compliance to the federal and state law enforcement mission. In order to receive authorization to share information, the use of the information must be compatible with the purpose for collecting the information as documented in the PIA and SORN. Each request for authorization covers a specific information sharing transaction with a federal, state, local, tribal, or foreign agency. CBP prepared over 400 such authorizations during the reporting period, in addition to those instances of sharing covered by a MOU.

1. Searches of Electronic Devices

CBP and ICE may conduct border searches of electronic devices as part of CBP's mission to interdict and ICE's mission to investigate violations of federal law at and related to U.S. borders. CBP Officers and ICE Special Agents conduct border searches of electronic devices to determine whether a violation of U.S. law has occurred. These searches have been an integral part of CBP's and ICE's border security and law enforcement missions since the inception of their predecessor agencies the U.S. Immigration and Naturalization Service and the U.S. Customs Service. In an effort to provide greater transparency, DHS Headquarters, the DHS Privacy Office, CBP, and ICE have undertaken a PIA that assesses the program in light of the FIPPs to discuss the relative rarity of these searches and the safeguards in place to protect the privacy of travelers subject to such a search. The PIA will be issued during the next reporting year.

To place the practice in perspective, between October 1, 2008 and May 5, 2009, CBP encountered more than 144.4 million travelers at U.S. ports of entry. Of these travelers, approximately 3.1 million (2.2% of the 144.4 million travelers) were referred to secondary inspection; however, CBP only conducted 1,947 searches of electronic media during this time period. A "search" in this regard may be as simple as turning on the device to ensure it is what it purports to be. Detailed information on these searches is only available for those performed on

laptops. Of the total number of searches of electronic media, only 696 (0.022% of the 3.1 million travelers referred to secondary inspection) were performed on laptops, which does not necessarily involve an in-depth search of the device. Of the 696 travelers subject to laptop inspection, officers conducted in-depth searches of 40 laptops.

2. Electronic System for Travel Authorization (ESTA)

CBP and the DHS Screening Coordination Office (SCO) worked to implement the Electronic System for Travel Authorization (ESTA) as a an alternative and eventual replacement for the I-94W, the Notice of Arrival and Departure for visitors from Visa Waiver Program (VWP) countries. ESTA is a requirement of the 9/11 Commission Act, section 711, which calls for the creation of an advanced electronic travel document for persons traveling under the Visa Waiver Program. CBP developed the program and DHS published both a SORN[77] and PIA[78] to provide privacy compliance prior to its January 12, 2009, mandatory implementation.

B. FEMA

FEMA's mission is to support citizens and first responders, ensuring that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

Over the course of the reporting period, FEMA undertook several privacy training initiatives. FEMA updated its privacy awareness training for new employees. Several other privacy initiatives are currently under development, which include: (1) advanced privacy awareness training for all employees; (2) a compliance training module on writing PTAs, PIAs, SORNs, and Privacy Act Statements; and (3) a privacy desk reference guide for employees focusing on compliance, education and training, incident response, and mitigation. Privacy awareness training will equip employees with increased awareness in regards to safeguarding PII as they fulfill FEMA's mission to provide assistance to individuals affected by emergencies and disasters.

Looking ahead, FEMA's privacy awareness and training efforts will include hosting an agency "Privacy Day" focusing on specific FEMA scenarios that showcase potential incidents involving PII. FEMA will also use its employee newsletter, *FEMA Forward*, to disseminate privacy awareness materials and educate employees on their PII responsibilities. Since July 2008, FEMA has undertaken a series of initiatives designed to improve privacy compliance, risk management, and privacy awareness. The details of FEMA's activities are discussed below in greater detail.

Due to the effect of natural disasters and other hazards directly upon individuals, FEMA routinely collects PII on applications submitted by survivors seeking assistance. The compliance process serves as a mechanism to improve public awareness of FEMA's information collections. From July 1, 2008, through June 30, 2009, the DHS Privacy Office worked closely with FEMA to significantly increase its FISMA compliance percentages. By completing 33 PTAs, 12 PIAs, and 7 SORNs, FEMA raised its FISMA scores for both PIAs and SORNs.

[77] http://edocket.access.gpo.gov/2008/pdf/E8-12789.pdf.
[78] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_esta.pdf.

In addition to its privacy compliance efforts, FEMA implemented risk management enhancements over the course of the reporting period. In accordance with OMB guidance and the *DHS Privacy Incident Handling Guide* (PIHG), FEMA has developed its PII Incident Standard Operating Procedures (SOP) to ensure timely response, coordination, and handling of privacy incidents, thereby lowering the risk of potential harm to affected individuals. FEMA has developed a tracking mechanism to identify trends that may exist among incidents. The result of analyzing such trends enhances FEMA's ability to mitigate risks and enhance the protection of PII.

C. ICE

ICE's mission is to protect national security by enforcing U.S. customs and immigration laws. ICE established its Privacy Office in April 2008 with the selection of its first Privacy Officer. The ICE Privacy Office consists of three federal personnel and several contractor staff. The office is in the process of hiring two additional federal positions.

During the past year, ICE focused on raising privacy awareness among its employees and contractors. All ICE personnel receive privacy and IT security training annually as part of ICE's online Information Assurance Awareness Training (IAAT). This training included modules on protecting information systems from unauthorized access; maintaining the confidentiality of sensitive information, including PII; recognizing and avoiding security threats at home and while traveling; and recognizing and reporting a security incident, including a loss or compromise of PII. The ICE Privacy Office also published bi-weekly privacy tips in the agency's electronic newsletter, which all employees and contractors received by email. ICE privacy tips provide helpful information to personnel on a range of privacy concerns, including the identification, protection and disposal of sensitive PII, and information about how to report privacy incidents.

Through its Privacy Office, ICE continues to improve the transparency of ICE operations and to ensure compliance with the Privacy Act and E-Government Act. During the reporting period, ICE completed three PIAs (working with the DHS Privacy Office) and has many more currently in progress. As part of a DHS-wide effort to update and consolidate legacy SORNs, ICE updated and republished six legacy SORNs from the former Immigration and Naturalization Service and the U.S. Customs Service. ICE also issued two new SORNs during the reporting period. Of particular interest was the publication of the PIA for the ICE Data Analysis and Research for Trade Transparency System (DARTTS) and the accompanying SORN, which were published in October 2008.

In support of ICE's law enforcement mission, DARTTS analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering, contraband smuggling, trade fraud, and other import-export crimes. These anomalies are then independently confirmed and further investigated by experienced ICE investigators. Because the analytical capabilities of DARTTS met the definition of data mining, DARTTS was also included in the DHS Privacy Office's 2008 Data Mining Report to Congress.

D. S&T

As the primary research and development arm of DHS, S&T conducts research related to preventing or mitigating the effects of catastrophic terrorism working in partnership with the private sector and other government agencies to encourage innovation in homeland security

research and technology development. S&T's research programs encompass a wide range of activities, from biological research on animal disease, to social-behavioral research on motivations for terrorism, to the development of new physical screening technologies. When an S&T research project involves or impacts PII, the DHS Privacy Office works closely with S&T to ensure the project is compliant with DHS privacy policy. As discussed in Section X.A of this report, S&T and the DHS Privacy Office jointly developed *Principles for Implementing Privacy Protections in S&T Research*, which serve as the framework for analyzing and addressing the privacy implications of S&T research projects.

In November 2008, S&T hosted an education and outreach workshop for the DHS Privacy Office in which representatives of each S&T research division briefed DHS Privacy Office staff on research areas and major ongoing or planned research projects. This workshop provided an opportunity for the DHS Privacy Office staff to ask questions about S&T research programs, practices, and policies, and provided another forum for collaboration.

S&T also arranged for the DHS Privacy Office to deliver S&T-specific training on preparing PIAs. The training session focused specifically on drafting PIAs for research, development, testing, and evaluation projects. During the workshop, the DHS Privacy Office provided guidance to S&T Program managers on when and why a PIA is required and how to complete a PIA that communicates program and project objectives effectively to the public. The workshop also provided an opportunity for the DHS Privacy Office to address S&T Program Managers' questions regarding PIAs and the PIA approval process.

S&T chairs a Privacy Working Group for the Identity Management sub-Integrated Product Team (IdM sub-IPT) to assess DHS components' capability gaps and research needs for privacy enhancing technologies. The working group members include ICE, the US-VISIT program, USCIS, TSA, FEMA, and I&A. As a result of working group discussions, S&T will initiate research and development efforts to explore data anonymization tools and techniques for testing and training purposes.

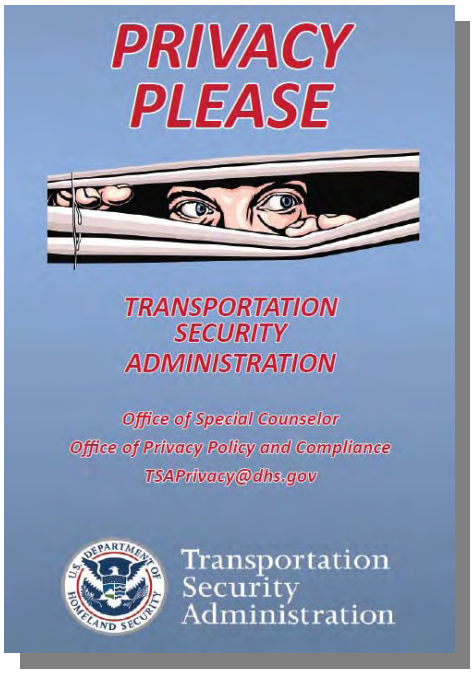
E. TSA

The Transportation Security Administration was created in the wake of the terrorist attacks of September 11, 2001, and is responsible for protecting the nation's transportation systems to ensure freedom of movement for people and commerce. TSA is most visible through its airport security screening efforts at more than 460 airports, but also has security roles in other modes of transportation.

1. Outreach and Awareness

The TSA Privacy Office took a variety of steps aimed at raising privacy awareness with internal and external audiences. The Office issued two new privacy awareness posters in its popular "Privacyman" series. The posters are designed to provide a short privacy message and point employees and contractors to available resources for more information. The posters addressed encryption of sensitive PII and the mechanics of reporting

data incidents. The office also created a "Privacy Please" door hanger similar to that found in hotels, with privacy tips on the reverse and office contact information.



Other internal outreach activities included speaking at a variety of employee meetings, such as the Town Hall meetings for employees within the Office of Acquisition, Human Resources monthly teleconferences, Threat Assessment manager meetings, and meetings with the Business Management Officers for each business unit within TSA. The TSA Privacy Office generated five broadcast email messages to its employees on a variety of topics throughout the year, and maintained an internal website with privacy resources for its employees. Topics for the e-mail broadcasts included cyber crime avoidance, restricting access to shared drives, taking care when addressing e-mail, updating the TSA Management Directive on handling sensitive PII, and limiting access to data to official purposes. The TSA Privacy Office also inserted privacy messages in the "remarks" field of the Statement of Earnings and Leave sent to every employee. The messages reminded employees of the obligation to protect data and provided the office contact information. The TSA Privacy Office also continued its news clipping "Privacy Awareness Press" series, issued periodically to sensitize program managers on privacy issues that have received media attention.

External outreach included speaking engagements at public conferences, such as a panel on Behavior Detection programs at the 2009 Computers Freedom and Privacy conference, a briefing on TSA programs and privacy efforts at two meetings of the Privacy Coalition (a consortium of 43 advocacy groups), a panel on How to Build Privacy Awareness at the IAPP Practical Privacy Series: Government conference, and a panel on Privacy and Homeland Security at an American Bar Association Homeland Security Committee meeting. TSA Privacy also met with individuals from the privacy advocacy community throughout the year.

2. Internal Leadership

The TSA Privacy Office continues to enjoy direct access to TSA executive leadership, including weekly meetings with the TSA Administrator. As part of its on-going efforts to further embed privacy within TSA, the TSA Privacy Office secured a position on the TSA Deputies Council to increase its ability to influence TSA policy development. The TSA Privacy Office also continued its active role within the TSA Information Protection Oversight Board, an executive level body intended to take a holistic view on all agency information and data protection practices. The TSA Privacy Office secured a reviewing role for every acquisition impacting information technology, including services contracts. Because information technology is so ubiquitous, this affords the TSA Privacy Office an opportunity to catch programs early-on in a more systematic way than simply relying on program managers. In addition, the TSA Privacy Office engaged with the development of an Insider Threat Program regarding internal employee investigations.

3. Policy Development

The TSA Privacy Office played a significant role in the development of DHS privacy policies for handling PII, and provided significant support to the DHS Privacy Office's Data Extracts Working Group. TSA Privacy Office staff also wrote the contract clause on data protection and breach response obligations for use in contracts involving PII, which was submitted to the Civilian Agency Acquisition Council for consideration as a new government-wide federal Acquisition Regulation (FAR) contract clause.

4. Security Programs

Significant PIAs published last year with guidance from the DHS Privacy Office included the Secure Flight Program Final Rule[79] and the Screening of Passengers by Observation Techniques (SPOT) program.[80] The Secure Flight program went operational in early 2009 and is expected to be fully operational in 2010. It is designed to bring the federal government watch list matching functions currently performed by the airlines within the government. Dual benefits from the program are expected to be more consistent watch list matching and more consistent application of redress for those passengers mistaken for individuals on a watch list. The SPOT program is a behavior observation and analysis program designed to provide Behavior Detection Officers (BDOs) with a means of identifying persons who pose or may pose potential transportation security risks by focusing on behaviors indicative of high levels of stress, fear, or deception. It is designed to provide for a more active security posture than simply searching for prohibited items. Privacy protections include not collecting any PII unless the individual displays behaviors that rise to a level calling for law enforcement involvement.

Other TSA programs with heightened public interest include imaging technology programs designed to use millimeter waves or x-rays to search for threat items that might be secreted beneath clothing. TSA conducted a PIA, which described the protections discussed below.[81] These technologies represent security improvements that address non-metallic threats, including explosives. TSA took a number of steps to mitigate the privacy impact of this technology. TSA designed the program to provide for complete anonymity for the individual undergoing the scan by placing the officer viewing the scan in a windowless room remotely located to prevent them from viewing the individual undergoing the scan, disabling at the manufacturer any capability to store or retain an image, placing a blur over the facial image, and providing notice to individuals that they may decline the scan in favor of a physical pat-down. The physical pat-down is needed to provide the same level of threat detection provided by the imaging technology. TSA is working with technology providers to further anonymize images by converting them to an abstract image, such as a cartoon, to further address privacy concerns with the technology. These modified abstract images seek to provide enough information to effectively locate the threat on the individual's person without providing a detailed image of their physical attributes.

F. USCG

The USCG's mission is to protect the public, the environment, and the U.S. economic security interests in any maritime region in which those security interests may be at risk. To protect and

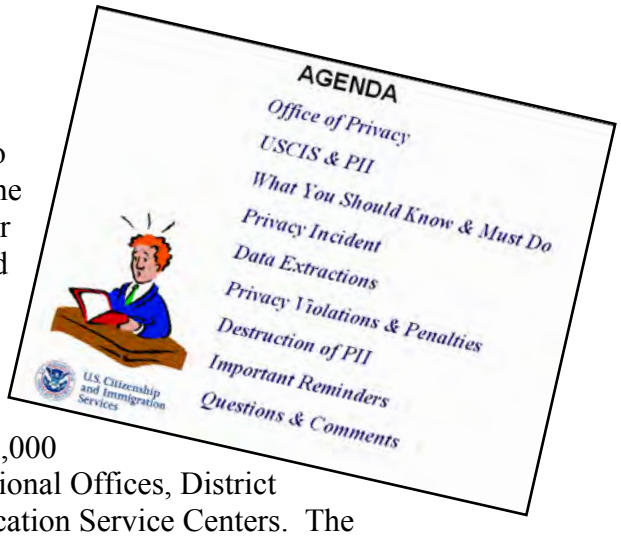
[79] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_secureflight2008.pdf.
[80] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_spot.pdf.
[81] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf.

promote privacy awareness, USCG Privacy Office staff delivered a presentation at the Annual Information Systems Security Officers (ISSO) Conference in Atlanta, GA, on March 31, 2009. More than 150 USCG ISSOs, Designated Approving Authorities (DAAs), and Information Assurance (IA) personnel attended this week long conference. The privacy presentation provided attendees detailed information relative to privacy incident reporting, Privacy Compliance Documentation (e.g., PTAs, PIAs, and SORNs), and C&A requirements. Presenters also reviewed current USCG and DHS privacy policies, as well as upcoming proposed policy changes. Handouts containing a comprehensive list of available resources proved invaluable. As a direct result of the information received at this conference, several ISSOs returned to their areas of responsibility and initiated process and procedural modifications to improve safeguarding PII. Conference attendees represented Information System Security Offices throughout the USCG, which has more than 40,000 personnel.

During September 2008, the USCG Privacy Office conducted Incident Reporting and Safeguarding PII training at the Coast Guard Assignment Officers Conference in Arlington, VA. The Assignment Officers are responsible for coordinating transfers, special assignments, separations, and retirements for 33,000 active duty and reserve Coast Guard personnel. They routinely counsel Coast Guard commands and members on various aspects of the assignment process and are instrumental in developing policies and procedures. Additionally, their duties require interfacing with various Human Resource systems and medical documents containing sensitive PII to determine suitability for assignments. Information presented by the USCG Privacy Office was instrumental in creating a heightened awareness of the importance of safeguarding PII for attendees.

In an ongoing commitment to provide public notice and agency transparency, the USCG published 21 SORNs in the Federal Register. This effort required collaboration between program managers, general counsel, the DHS Privacy Office, DHS Headquarters, and various field offices. The USCG Privacy Office conducted a thorough review of all missions to ensure compliance with current federal mandates and requirements. Moreover, during this endeavor, USCG consolidated 13 systems for efficiency, retiring five SORNs which were subsumed into other program areas.

G. USCIS



USCIS is responsible for overseeing lawful immigration to the U.S. and preserving America's legacy as a nation of immigrants while ensuring no one is admitted who is a threat to public safety. The USCIS Office of Privacy made training the number one priority this year. USCIS believes the best and most efficient way to ensure all staff and contractors are equipped to perform their duties and ensure public trust is not lost is to train 100% of its staff. By the end of FY 2009, USCIS Office of Privacy will have trained over 18,000 federal employees and contractors throughout Regional Offices, District Offices, Field Offices, Asylum Offices, and Application Service Centers. The

USCIS Office of Privacy administered instructor-led training, as well as the DHS Privacy Office's *Culture of Privacy Awareness* computer-based training.

USCIS Office of Privacy extended its outreach training efforts to Congressional staffers, providing them with an in-depth privacy presentation depicting USCIS staff responsibilities as it pertains to responding to Congressional inquiries. Additionally, the USCIS Privacy Officer recently disseminated a memorandum, *USCIS Policy Regarding Personally Identifiable Information,* to all USCIS employees and contractors, to ensure staff clearly understood what information could be sent within the DHS firewall unencrypted and what information requires encryption.

USCIS Office of Privacy has grown since last year. The Office has three full time employees (FTEs) and will hire another FTE during the next reporting period. USCIS Office of Privacy hired an Administrative Program Management Analyst to handle all administrative matters for the USCIS Office of Privacy and to play a key role on the Privacy Training team. USCIS will also add a Senior Privacy Analyst. This staff member will be the primary liaison between the Office of Privacy and the USCIS Office of Information Technology (OIT) in all OIT and privacy matters. The staff member will ensure all IT systems are updated in a timely manner and will review all privacy related documents before they are reviewed by the USCIS Privacy Officer. Most importantly, this staff member will play a major role in the USCIS transformation process. Currently, USCIS processes and systems do not allow the component to meet modern immigration demand. To meet the demands of transitioning USCIS from a fragmented, paper-based operating environment to an electronic, account-based person centric operating environment, USCIS has begun the transformation process.

One of the major internal areas of focus for USCIS is the agency-wide organizational and business transformation initiative (Transformation), which includes a large IT systems modernization effort. Transformation will benefit USCIS in many ways. Specifically, it will help USCIS establish an electronic end-to-end adjudication solution that will bring systemic changes to how USCIS conducts business, improving not only the accuracy and speed of adjudication but providing increased security and identity management. These efforts will also eliminate the elaborate and time consuming receipt, intake, shipping, and tracking processes. The USCIS Office of Privacy must have a presence in all relevant Transformation meetings and discussions to ensure privacy is built into the Information Technology Life Cycle Management System (ITLMS) for all USCIS IT systems. USCIS plans to hire a senior level Privacy Analyst to assume these responsibilities. This individual will also advise the USCIS Privacy Officer on key issues regarding transformation, hold meetings as needed, take on the responsibilities of the USCIS Deputy Privacy Officer in her absence, and work closely with the DHS Privacy Office to ensure that privacy protections are built into USCIS IT systems.

H. USSS

In an effort to promote a culture of privacy awareness, USSS implemented a mandatory privacy awareness training course which is available via electronic media within the USSS Learning Management System. The course provides a basic overview of federal privacy laws, including the Privacy Act, FOIA, and the E-Government Act. The course also covers rules for handling PII and data breaches. USSS employees and contractors are required to take the course annually. Over 6,000 instances of training were provided during this reporting period.

In collaboration with the DHS Privacy Office, USSS Systems Managers, and Program Managers, the USSS reviewed and updated all legacy SORNs. In an effort to streamline DHS SORNs, several USSS legacy SORNs were consolidated into DHS-wide SORNs. The USSS SORNs were streamlined from seven to three major SORNs. Approximately 17 USSS systems of records were consolidated into DHS-wide SORNs. Three notices of proposed rule making (NPRMs) relating to exemptions for the SORNs were reviewed and submitted to the DHS Privacy Office for issuance and publication. This collaborative effort has promoted and improved transparency and privacy compliance within the USSS.

Concurrent with the increase of responsibilities, the Secret Service's Deputy Director has allocated a staffing increase to support the program efforts to ensure compliance with the Privacy Act, FOIA, the E-Government Act, and other privacy compliance requirements. The program is in the process of recruiting a Privacy Compliance Specialist. The Secret Service is also recruiting several FOIA/PA Specialists.

I. US-VISIT

The mission of US-VISIT's Privacy Office is to uphold the privacy of individuals while protecting the Nation's borders.[82] This is achieved by adhering to the letter and spirit of U.S. privacy law, complying with the FIPPs, treating individuals and their PII with respect, and ensuring high standards of privacy protection.

US-VISIT fosters a culture that values protecting information. The program office has a full-time Privacy Officer and a team of privacy analysts who are responsible for ensuring compliance with all applicable privacy laws, regulations, and internal privacy requirements. The privacy program actively builds and supports a workplace culture that values privacy by providing employees and contractors with job-related privacy training and annual privacy refresher training. In addition, the US-VISIT Privacy Officer and the privacy team are involved in new projects from the earliest stages through the execution stage, and continuing for the duration of the project's operations and maintenance to ensure that privacy standards are in place.

1. Conducting Privacy Impact Assessments

During the reporting period, the US-VISIT privacy program continued to demonstrate a strong commitment to privacy protection by publishing four PIAs in collaboration with the DHS Privacy Office. In October 2008, US-VISIT published a PIA that described the first phase of interoperability between US-VISIT and the Criminal Justice Information Services Division of DOJ.[83] In February 2009, US-VISIT published a PIA to inform the public about the enrollment of additional aliens in US-VISIT.[84] Both PIAs outlined all associated privacy risks and the safeguards that were implemented to mitigate those risks. In May 2009, US-VISIT published a PIA for the Comprehensive Air Exit pilot to assure the traveling public that strong physical, administrative, and technical safeguards protect the confidentiality, integrity, and availability of exit information.[85] US-VISIT is currently engaged in conducting updated PIAs for its Arrival

[82] More information about the US-VISIT culture of privacy and the privacy program is available on the US-VISIT website at http://www.dhs.gov/xtrvlsec/programs/gc_1180020923182.shtm.
[83] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_phase1ioc.pdf.
[84] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addl%20aliens.pdf.
[85] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_air_exit.pdf.

and Departure Information System (ADIS)[86] and Automated Biometric Identification System (IDENT).[87]

2. Data Sharing Within DHS and Other Government Agencies to Meet Mission Needs

US-VISIT, in cooperation with the DOJ Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division, implemented the first phase of initial system interoperability between US-VISIT and CJIS. This interoperability expands upon and improves the method by which certain biometric and biographic data are exchanged and shared, and increases data sharing between DHS and federal, state, and local law enforcement agencies regarding activities related to the DHS mission. A PIA published in October 2008 describes the uses and sharing of information under the first phase of the system's interoperability, as well as the associated privacy risks and measures taken by US-VISIT to mitigate those risks. As with all information sharing protocols, US-VISIT maintains the highest standards of security and privacy protection in relation to the information

3. Forei gn Government Outreach

US-VISIT actively supports the DHS Privacy Office's international outreach efforts by working with foreign government officials interested in learning about biometric identity management, and establishing data sharing agreements that help facilitate the timely entry and exit of visitors. US-VISIT has begun limited exchanges of immigration fingerprint records with foreign government participants to explore the feasibility and value of routine information sharing. Such collaboration on fingerprint data sharing has delivered the following key benefits to DHS and its foreign partners:

- Enhanced integrity of the U.S. border management and immigration system through positive identification of known or suspected criminals, terrorists, and immigration violators;
- Improved public safety by ensuring that persons with known criminal histories (or who pose other risks) are identified during the immigration process; and
- Early identification of ineligible immigration applicants, which has reduced operational costs within the respective countries while also facilitating legitimate travel and trade.

While engaging in these data sharing efforts, US-VISIT employs specific measures to protect the privacy of individuals including:

- Using encryption and other security tools to protect files that are shared; and
- Publishing a comprehensive PIA and consulting with each participating country's official responsible for the oversight of privacy matters.

[86] The current ADIS PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_adis_2007.pdf;
[87] The current IDENT PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_enumeration.pdf.

XII. Preventing and Managing Privacy Incidents

A. New Position: Director, Privacy Incidents and Inquiries

The DHS Privacy Office continues to excel in its mission to sustain privacy protections and promote transparency of operations while achieving the Department's goals. In November 2008, the DHS Privacy Office hired a Director of Incidents and Inquiries to manage the Office's growing incident response and complaints program. The Director and staff, now known as the Incidents and Inquiries Group, have become an integral part of DHS Privacy Office operations. The Director is responsible for the Privacy Incident Management program through collaboration with the DHS Enterprise Operations Center (EOC), component Privacy Officers and PPOCs, and DHS management. The Director ensures incidents are properly reported and that mitigation and remediation efforts are appropriate for each incident.

B. Collaboration with Components

The Director of Incidents and Inquiries and her staff have coordinated and collaborated with each component to manage and monitor incidents. The Incident and Inquiries Group met with six DHS components to determine how they are managing privacy incidents, safeguarding PII, and addressing other privacy issues. The staff assisted the components in identifying trends of privacy incidents, discovering areas of vulnerability, and ultimately preventing the likelihood of future occurrences. The visits provided each component the opportunity to raise potential issues and discuss resolutions in a collegial environment. The component visits also enabled the DHS Privacy Office to observe how the components incorporate privacy protection into all aspects of their mission. The DHS Privacy Office developed training based on the lessons learned during these visits, which has led to increased awareness and prevention of privacy incidents.

C. DHS Privacy Incident Response Plan

The DHS Privacy Office worked steadily over the past two years to continue implementation and revision of the PIHG, the cornerstone of privacy incident policy within DHS.[88] The PIHG informs DHS components, employees, and contractors of their obligation to protect the PII they are authorized to handle and explains how to respond to suspected or confirmed privacy incidents. The PIHG strictly adheres to OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* issued on May 22, 2007 (OMB M-07-16),[89] which is the foundation for the management of all privacy incidents across the federal government.

[88] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.
[89] http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

DHS has a legal obligation to safeguard PII and implement procedures for handling both privacy and computer security incidents. The DHS Privacy Office is the lead office for implementation of the privacy incident response program throughout the Department. Privacy incidents can occur within both the unclassified and classified realm of information at DHS. Strict adherence to the DHS Sensitive Systems Handbook and Policy (DHS Directive 4300), as well as the CISO Continuity of Operations (CONOPS), enables the DHS Privacy Office and the CIO/CISO to monitor and mitigate all types of privacy and security incidents. Through continued close collaboration, the DHS Chief Privacy Officer, the CIO, the CISO, and EOC ensure that all of the Department's privacy and computer security incidents are identified, reported, and responded to appropriately 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 consistent manner.

During the reporting year, the DHS Privacy Office continued to refine its privacy incident management program. The DHS Privacy Office developed and published a "Desktop" PIHG that has been used as a quick reference guide by ISSMs, component Privacy Officers and PPOCs, and individual information system program managers. The Desktop User's Guide was published on September 28, 2008 and will be posted to the DHS Privacy website with the PIHG in September 2009.

A total of 351 privacy incidents were reported to the DHS EOC during the reporting period. The majority of the incidents affected a small number of individuals and data, while a select few of the incidents consisted of large amounts of data. Mitigation and remediation of each incident is a coordinated effort among the DHS Privacy Office, EOC, component Privacy Officers and PPOCs, and ISSMs. Without this collaborative effort, DHS would not be able to respond effectively and completely to the privacy incidents. Of the reported privacy incidents, DHS investigated, mitigated, and closed 270, representing 77% of the total incidents. The average number of open days for an incident has increased from 32 days in the previous reporting period to 46 days during the current reporting period. This increase in the number of open days per incident is due to the increased number and complexity of incidents reported. **Table 1** depicts the number and type of incidents reported during the past two years.

Type of Incident[90]	Number of Incidents: July 1, 2008 to June 30, 2009	Number of Incidents: July 1, 2007 to June 30, 2008
Alteration/Compromise of Information[91]	296	147
Classified Computer Security Incident[92]	12	1
Investigation Unconfirmed/Non-Incident[93]	18	14

[90] Types of incidents are detailed in Federal Information Processing Standards (FIPS) 200 and NIST SP 800-53.
[91] **Alteration/ Compromise of Information** - This includes any incident that involves the unauthorized altering of information, or any incident that involves the compromise of information.
[92] **Classified Computer Security Incident** - Any security incident that involves a system used to process national security information. (NOTE: None of the 12 incidents involved a breach of a classified system, rather the incidents involved classified data "spilled" on unclassified systems. For example, classified information introduced to a computer system/device that did not have the appropriate classification level or transmitted without appropriate protection.)
[93] **Investigation Unconfirmed/Non-Incident** - This includes all successful unauthorized accesses and suspicious unsuccessful attempts and suspected but unconfirmed incidents.

Type of Incident[90]	Number of Incidents: July 1, 2008 to June 30, 2009	Number of Incidents: July 1, 2007 to June 30, 2008
Malicious Logic[94]	4	2
Misuse[95]	15	32
Unauthorized Access (Intrusion)[96]	6	5
Total	***351***	***201***

Table 1: DHS Privacy Incidents Reported

The privacy incident handling process at DHS continues to evolve. This program has been emulated by various federal agencies throughout the government and was identified as one of the most integrated and robust systems within the federal space.

D. Collaboration with DHS EOC

Close communication with the DHS EOC has yielded an efficient and effective reporting system with a high level of trust between the DHS Privacy Office and the DHS EOC analysts in charge of the incident reporting process. This allowed the DHS Privacy Office to request modifications to the online reporting process to reflect lessons learned and new capabilities, as well as to obtain reporting capabilities that provide key metrics for the program. The Incidents and Inquiries Group visited the DHS EOC and gained additional knowledge of the staffing structure, mission, and vision. The DHS Privacy Office was instrumental in assisting the EOC in identifying an appropriate software tool to completely erase unauthorized data from all DHS IT assets. The DHS Privacy Office also learned more about the intrusion detection and protection software EOC was testing to monitor all DHS IT traffic transmitted via the DHS Intranet through an EOC staff demonstration. The visit allowed the DHS Privacy Office to show its appreciation to the DHS EOC staff for their commitment and contribution to the Department's collective effort to prevent privacy incidents. Privacy staff also attend the EOC/CISO joint quarterly meetings and have provided in depth briefings at these meetings.

E. Annual Core Management Group Meeting

OMB M-07-16 and the PIHG call for a Core Management Group and require yearly meetings of DHS executive management to evaluate and discuss privacy incidents and incident handling procedures. The DHS Core Management Group consists of the following: Deputy Secretary, Chief Privacy Officer, CIO, the Office of General Counsel, OIG, CSO, the Public Affairs Office, the Legislative and Inter-Governmental Affairs Office, the Management Office, Chief Financial Officer (CFO), component IT Security entities, and component Privacy Officers and PPOCs. The DHS Privacy Office convened the first DHS Core Management Group in July 2009; this and other future additions to our incident program will be discussed in the next reporting year.

[94] **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.

[95] **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.

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

XIII. Complaints

A. Managing Complaints

The new Director of Incidents and Inquiries has responsibility for reviewing privacy complaints received throughout the Department and components, including complaints received from the general public, non-profit organizations, and self-regulatory organizations. This position provides the DHS Privacy Office a dedicated resource to support complaint-handling as a team leader, team member, or sole investigator for the most difficult, sensitive and complex privacy investigative matters.

B. 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. As part of its quarterly FISMA reporting, the DHS Privacy Office is now required to report to Congress the number and types of privacy complaints received throughout the Department.

Section 803 complaints are separated into four categories: (1) process and procedure, (2) redress, (3) operational, and (4) referred. As reporting is further developed, additional categories may be added.[97]

- **Process and procedure.** Issues concerning process and procedure, such as consent, notice at the time of collection, or notices provided in the Federal Register, such as rules and SORNs.

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

- **Redress.** Issues concerning appropriate access, correction of PII, and redress therein.

  Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[98]

- **Operational.** Issues related to general privacy concerns and concerns not related to transparency or redress.

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

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

[97] During the FY2008 Q4 reporting period, DHS updated its categories to match the categories required for Federal Information Security Management Act (FISMA)/Privacy Reporting described in OMB's Memorandum M-08-21. Based on these changes, "Referred" complaints are now counted separately. In previous reports, "Referred complaints" were categorized as a responsive action.

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

- **Referred.** The 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.

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

Complaints are also analyzed according to their disposition. Complaints are classified in one of four categories: (1) responsive action taken, (2) referred, (3) no action required,[99] and (4) pending. The categories are defined as follows:

- **Responsive Action Taken.** The 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.
- **No Action Required.** The 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 the individual is upset because of the length of wait time at an airport security checkpoint.
- **Pending.** The component or the DHS Privacy Office is reviewing the complaint to determine the appropriate response.

The following table provides the figures reported to Congress and OMB during the reporting period between June 1, 2008, and May 31, 2009.[100] A cornerstone of the DHS complaint system is the definition of "complaints" set by OMB, which defines them as written allegations of harm or violation of privacy compliance requirements.[101] These reports reflect privacy complaints filed with the DHS Privacy Office and components or programs. Complaints may be from U.S. citizens and lawful permanent residents, as well as visitors and aliens.[102] **Table 2** summarizes the categories and disposition of complaints received during the past four quarters. It is important to note that the number of pending "process and procedure" complaints reflects 2,012 complaints received as part of a fourth quarter FY 2008 write-in campaign regarding laptop searches. DHS plans to issue a PIA regarding laptop searches that will discuss updated DHS policies regarding them. These complaints will be reclassified as "responsive action taken" after the PIA has been published, as the complaints sought to influence policy regarding laptop searches as opposed to individual redress.[103]

[99] The complaint disposition classification "no action required" was previously labeled "unable to assist."
[100] The reporting period for June 1, 2009 through August 31, 2009 was on-going at the close of the reporting period for the Privacy Office Annual Report.
[101] OMB-08-09.
[102] 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.
[103] The Commissioner of CBP received 2,012 email messages (form letters) regarding the search of electronic devices policy expressing objections to such searches. The DHS Privacy Office determined these messages should be reported as complaints. The electronic devices PIA, which will be issued later this year, will address the issues raised in these complaints. See CBB for more details.

Privacy Complaints Received with Action Taken

Type of Complaint	Number of Complaints	Disposition of Complaint		
		Responsive Action Taken	No Action Required	Pending
Fourth Quarter FY 2008 (June 1, 2008 - August 31, 2008)				
Process and Procedure	2,020	8	0	2,012
Redress	480	331	149	0
Operational	14	13	0	1
Referred	46	46	0	0
Total	***2,560***	***398***	***149***	***2,013***
First Quarter FY 2009 (September 1, 2008 - November 30, 2008)				
Process and Procedure	1	1	0	2,012
Redress	242	62	0	182
Operational	35	2[104]	0	34
Referred	36	36	0	0
Total	***314***	***101***	***0***	***2,228***
Second Quarter FY 2009 (December 1, 2008 - February 28, 2009)				
Process and Procedure	32	6	26	2,012
Redress	70	44	0	27
Operational	8	4	2	3
Referred	14	14	0	0
Total	***124***	***68***	***28***	***2,042***
Third Quarter FY 2009 (March 1, 2009 - May 31, 2009)				
Process and Procedure	1	1	0	2,012
Redress	322	228	0	121
Operational	8	7	2	3
Referred	40	40	0	0
Total	***371***	***276***	***2***	***2,136***

Table 2: DHS Privacy Complaints Received by Quarter

C. Component Complaint Handling

Below are some examples of component responses to complaints received from July 1, 2008 through June 30, 2009. Collaboration among the DHS Privacy Office and components was a major contributing factor to the successful resolution of the complaints.

1. ICE

During the past year, the ICE Privacy Office received nearly 20 privacy complaints from members of the public. Several of the complaints concerned allegations that illegal aliens were using complainants' identities to obtain employment. The ICE Privacy Office referred these identity theft complaints to ICE field offices for appropriate resolution. Travelers also submitted complaints describing problems encountered while trying to travel to the U.S. These individuals often believed a mistake was made during screening at the port of entry. Individuals who submitted such complaints were directed to DHS TRIP for redress.

[104] This number includes a complaint that was pending from fourth quarter FY 2008.

The ICE Privacy Office also received several complaints from ICE employees and contractors. These complaints pertained to specific instances where sensitive PII was perceived to be either maintained or collected in a manner that was intrusive or inconsistent with DHS privacy policies. For example, one person complained that the ICE IT helpdesk's electronic complaint system required users to provide the last four digits of their SSN when submitting trouble tickets. The ICE Privacy Office worked with the ICE Office of the Chief Information Officer to modify the system to eliminate use of the partial SSN as an identifier.

2. USCIS

During the past five years, USCIS has made appellate decisions publicly available. USCIS policy states that PII must be redacted before these documents are made available to the public. This practice prevents the exposure of personal information. Four years ago an individual appealed a decision after the denial of a benefit. In this case, the name of the complainant and his wife appeared in the document when USCIS made it publicly available. The complainant found his information using a web search with his name as the subject. He contacted the USCIS Privacy Office, which then contacted the appropriate USCIS office to delete the information. The responsive USCIS office also persuaded the commercial entities posting the appellate decision to remove the information. The complainant and his wife considered this a successful resolution of their complaint.

3. FEMA

In response to a FEMA PII incident notification letter, FEMA received a letter complaining about the unauthorized release of an individual's personnel SF-50 Notification of Personnel Action form. FEMA offered the affected individual an 18-month membership in an ID theft protection program and provided guidance to the individual on mitigating the potential impact of the disclosure. The complaint was resolved to the individual's satisfaction.

4. CBP

CBP has numerous legacy IT systems within its inventory, many of which have older menu driven systems that require SSNs for both user identification and, in conjunction with a password, user access. A significant and recurring privacy concern posed by these systems was the need to share an SSN to reactivate or restore a disabled password. While an immediate supervisor would have access to the SSN by virtue of her or his access to the employee's personnel and payroll records, there is little need to know the SSN beyond this context.

After consultation between the CBP Privacy Branch and the IT Systems Security Branch, a solution to the common practice of sharing one's SSN to restore a password was adopted. CBP expanded its use of a new certification system, delegated the authority to reset passwords for administrative and lack of use suspensions to the immediate supervisor, and adopted the use of a HASH ID (a weak, 7-digit, alphanumeric, algorithmic representation of the SSN) to identify the employee whose password was to be reset. While CBP acknowledges that this was not a perfect solution, it provided a significant measure of privacy to an employee's SSN without engendering a time-consuming and costly reprogramming of an older mainframe IT system.

D. Improving the Complaint Handling Process

The DHS Privacy Office is continuing to upgrade and standardize its complaint handling processes. To that end, the DHS Privacy Office is developing the Complaint Tracking System, an electronic complaint tracking system to address privacy complaints, respond to access requests, and provide redress as appropriate in a timelier manner. The new system is scheduled for implementation by September 2009. A PIA and a SORN will be published for the system at that time. In addition to providing greater efficiency to the complaint management process, the system will facilitate compiling quarterly data for the section 803 Reports described in Section XIII.B.

E. Response to Public Inquiries

In addition to complaints, the DHS Privacy Office receives hundreds of emails throughout the year requesting information or providing comments. The DHS Privacy Office provides an email address through its website at privacy@dhs.gov, which members of the public can use to contact the Office. However, the majority of emails received at this email address typically involve issues that are outside the DHS Privacy Office's area of responsibility. Such comments, complaints, and requests are referred to the appropriate component or other federal agency. Several examples of the emails received by the DHS Privacy Office this year are provided below.

- **Information about Name Changes –** A researcher studying the cancer burden of Latino populations in his state made an inquiry. Specifically, he inquired if there were any statistics regarding the percentage of voluntary name changes among those who receive U.S. citizenship at the time of naturalization.
- **Travel Documents –** An individual inquired about a situation where she could not find her passport at the time of departure from the United States. Upon arrival in her home country, the individual found her passport. She stated "I could [travel] back home with my ID, but as I did not have my passport with me, I could not give back this green paper attached into my passport when I entered into the US." The individual asked about the best method to send this travel documentation to the U.S. in order to avoid future travel problems.
- **Fake Identity Sales –** An individual informed the DHS Privacy Office about the sale of identity information and documents to immigrants for the purpose of obtaining visas.
- **Privacy Policy –** An individual informed the DHS Privacy Office about his or her opinion that the privacy policy for a city program using DHS funding did not meet DHS privacy best practices.
- **Border Entry –** An individual asked for assistance regarding border crossing. Two of this individual's associates were denied entry into the U.S. This individual believed that there was no reason for this denial.
- **Fake Immigration Documents –** An individual informed the DHS Privacy Office about restaurant workers using fraudulent documentation to obtain green cards.

- **Identity Theft –** An individual informed the DHS Privacy Office about a person using another person's information to obtain employment. This information included the person's name and SSN.
- **Fraudulent Marriage –** The DHS Privacy Office received an inquiry providing information about a person attempting to obtain a green card through false marriage.

XIV Reporting and Inquiries

A. 9/11 Commission Act Section 803 Reporting to Congress

In addition to reporting on complaints, section 803 of the 9/11 Commission Act created new quarterly reporting requirements for select privacy offices within the federal government, including the DHS Privacy Office. Each section 803 report submitted contains information regarding: (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.

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

- Privacy Threshold Analyses;
- Privacy Impact Assessments;
- SORNs and associated Privacy Act Exemptions;
- Privacy Act (e)(3) Statements;
- Computer Matching Agreements; and
- Privacy protection reviews of IT and Program Budget requests, including OMB 300s and Enterprise Architecture Alignment Requests through the DHS EAB.

The Chief Privacy Officer submitted the four quarterly reports required under section 803 of the 9/11 Commission Act during this reporting period. Copies of these reports are available on the DHS Privacy Office website.[105] The following sections contain the information reported by DHS during the past year for each activity listed above.

1. Activities Reported

Table 3 provides the number of completed section 803 activities for each type of review completed by DHS June 1, 2008 through May 31, 2009.

Type of Review	Number of Reviews
Privacy Threshold Analyses	407
Privacy Impact Assessments	65
System of Records Notices and associated Privacy Act Exemptions	124
Privacy Act (e)(3) Statements	8
Computer Matching Agreements	5

[105] http://www.dhs.gov/xinfoshare/publications/editorial_0514.shtm#3.

Type of Review	Number of Reviews
Data Mining Reports	1
Privacy Protection Reviews of IT and Program Budget requests	122
Total Reviews Completed June 1, 2008 through May 31, 2009	***732***

Table 3: DHS section 803 Reviews Completed June 1, 2008 through May 31, 2009

2. Advice and Responses

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

- *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*, October 2008;
- *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008; and
- *Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments*, December 30, 2008.

During the reporting period, DHS conducted the following training:

- DHS personnel and contractors attended classroom-based privacy training courses in 9,013 instances.
- DHS personnel and contractors completed computer-assisted privacy training courses in 96,012 instances.

Additional component activities are described in Section XI of this report.

Section 803 Reports regarding complaints received by the DHS Privacy Office and components are provided in Section XIII of this report.

B. FOIA Reporting to the Attorney General and Compliance

DHS programs and policies continue to be the subject of numerous FOIA requests due to high public interest in the Department's operations. The DHS FOIA Program is centralized for the purpose of establishing policy, but is managerially and operationally decentralized in each component. The DHS FOIA Program consists of 267 full-time and 52 part-time FOIA and Privacy Act personnel, costing an estimated $24 million in FY 2008. Incoming requests totalled 109,952 in FY 2008, while the Department processed 109,028 incoming requests and granted 68,368 requests in full or in part during that timeframe. The DHS Privacy Office FOIA staff received 849 initial requests in FY 2008, including 107 complex cases, requiring searches and coordination from multiple components.

1. Compliance with Executive Order 13392 and President Obama's Transparency Initiatives

In response to the deliverables required by Executive Order 13392, the DHS FOIA Office 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. The revised FOIA Improvement plan also focused on particular components with large backlogs. Of the 39 milestones listed in the 2007 Annual FOIA Report to DOJ, DHS fully met 29, with many of the remaining deficiencies pertaining to unique circumstances at individual components. In furtherance of the mandate to make FOIA programs more citizen-centered, the DHS FOIA Office continued to assess the staffing, technological, and educational needs of every DHS FOIA program. Additionally, the DHS Privacy Office sent monthly FOIA completion rates to all components to help them meet their FY 2009 backlog elimination goals.

In January 2009, the DHS Privacy Office drafted the Department's final FOIA regulations, which are currently being reviewed internally. These regulations outline the FOIA requirements and responsibilities for DHS and its components, and serve to educate the public about the impact of FOIA requirements on DHS and the proper procedures for filing a FOIA request. The regulations also provide detailed procedures governing the way DHS processes FOIA requests. The target date for publication of the Notice of Proposed Rulemaking is November 2009.

The DHS Privacy Office also issued updates to DHS FOIA policies and procedures to comply with the President's FOIA Memorandum, as well as implementation guidance issued by the Attorney General. These new policies reverse FOIA guidelines in place since 2001 and call for a presumption of openness which is the heart of the FOIA. In addition to revising policies and procedures, the DHS Privacy Office issued memoranda notifying DHS of the new FOIA requirements and urging component FOIA offices to comply with new FOIA guidance.

2. Compliance with the OPEN Government Act

The *Openness Promotes Efficiency in our National Government Act of 2007* (OPEN Government Act), signed by President Bush on December 31, 2007, amended FOIA and codified several 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. The OPEN Government Act also directed that court awarded attorneys' fees be paid from an agency's own appropriation, prohibited agencies from assessing certain fees if it fails to comply with FOIA deadlines, and established an Office of Government Information Services at the National Archives and Records Administration to review agency compliance with FOIA. Furthermore, the OPEN Government Act codified the role of the Chief FOIA Officer and FOIA Public Liaison. On February 5, 2008, the DHS Privacy Office 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 FY 2008 Annual FOIA Report to DOJ. Most notably, all components were required to report the number of times the component relied upon each b(3) (statutory specific) exception, the average and median initial

request and appeal response times, request counts by response times (how many within 0-20 days, 21-40 days, in 20-day increments up to 300 days and between 301-400 days), list the agency's ten oldest pending requests and appeals, account for requests seeking expedited treatment, accounting for all fee waiver assessment requests, and more detailed reporting of consultations received from other agencies. In an effort to ensure timely compliance, the DHS FOIA Office prepared briefings and outlines for each component to inform them of the new reporting requirements for the FY 2008 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. Each component submitted their draft information to the DHS Privacy Office to compile all individual data and prepare the overall report for the agency. The FY 2008 report was published to the DHS website January 16, 2009.

C. Data Mining Report to Congress

In December 2008, the DHS Privacy Office issued its 2008 report to Congress on DHS data mining activities as required by section 804 of the 9/11 Commission Act entitled the Federal Agency Data Mining Reporting Act of 2007 (Data Mining Reporting Act). The report, *Data Mining: Technology and Policy* (Data Mining Report), discusses DHS activities already deployed or under development that meet the Data Mining Reporting Act's definition of data mining. For each DHS program discussed, the report describes the program's purpose and methodology, technology employed, legal authority, and the sources of data used by the program. Each program description includes an analysis of the program's efficacy, concluding with a discussion of the program's impact on individual privacy and the protections in place to address those impacts. The Data Mining Report also provides a summary of the DHS Privacy Office's public workshop, Implementing Privacy Protections in Government Data Mining, held on July 24-25, 2008. The workshop was discussed in the *DHS Privacy Office 2008 Annual Report*.

The Data Mining Report also presents new privacy principles for research projects conducted by S&T. As noted earlier in Section X.A, the *Principles for Implementing Privacy Protections in S&T Research Projects* were developed jointly by the DHS Privacy Office and S&T, and will be implemented in all privacy-sensitive S&T research projects, including those that involve data mining.

D. CCTV

In December 2007, the DHS Privacy Office held a public workshop titled CCTV: Developing Privacy Best Practices. The workshop examined ways technology, local and international communities, law enforcement, government agencies, and privacy advocates can shape the use of CCTV and discussed the safeguards that should be in place as use of CCTV continues to expand. In January 2009, the DHS Privacy Office and CRCL published a report in December 2008 that summarizes the workshop panel discussions and provides resources to help identify and address privacy concerns.[106] The resources shared in the workshop report included Best Practices for Government Use of CCTV; a Template for Privacy Impact Assessment for the Use

[106] The report, *CCTV: Developing Privacy Best Practice, Report on the DHS Privacy Office Public Workshop,* is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.

of CCTV by DHS Programs; a Template for Privacy Impact Assessment for the Use of CCTV by State and Local Entities; and a Template for Civil Liberties Impact Assessments (CLIA).[107]

[107] *Id.*

XV. The Future of Privacy at DHS

The DHS Privacy Office continues to establish itself as an integral part of DHS; and as part of this evolution, it will continue to raise privacy awareness and encourage a culture of privacy throughout the Department. The Chief Privacy Officer intends to systematize privacy across the Department so that privacy is considered as a matter of course as components and the Department develop their systems and initiatives. The DHS Privacy Office will continue to serve as a resource for information and guidance and consistent policy approaches, while further serving as a leader on federal privacy policy.

The Chief Privacy Officer's goal of systematizing privacy throughout the Department can be accomplished in a variety of ways. First, the DHS Privacy Office is making training available in a variety of formats – in person classroom training, in-depth workshops, and online training. During the next year, the Office will look for other opportunities to provide privacy training through additional media and distribution channels. The Office will continue to leverage component training opportunities and seek to identify best practices in training. Second, the Office will participate in intra- and extra-Departmental working groups and committees, and lead the Department in international engagements regarding privacy matters.

The DHS Privacy Office expects new and challenging privacy issues will continue to emerge in cybersecurity, social media, immigration reform, and other areas. The Office intends to meet these challenges by regularly engaging the Department's leadership and working with component and program managers to ensure that privacy protections are implemented. Finally, by adding new component privacy officers and DHS Privacy Office positions, the Office will recruit professionals who can provide privacy expertise with program and technical knowledge. This confluence of high level strategic privacy policy coupled with on-the-ground, practical implementation of the FIPPs will provide a unique depth and breadth of privacy protections in the Department while further developing its culture of privacy.

XVI. Appendices

A. DHS Implementation of the FIPPs

DHS's implementation of the FIPPs[108] 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).
- 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.

[108] *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 29, 2008) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

B. Published PIAs

The table below lists all published PIAs between July 1, 2008 and June 30, 2009.

Component	Name of System	Date Approved
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
CBP	Operations at the Land Border	7/2/2008
S&T	REAL EYES	7/25/2008
FEMA	First Responder Training Portal (FRTP)	7/25/2008
TSA	Operations Center Incident Management System (OCIMS),	7/25/2008
S&T	Standoff Explosives Detection Technology Demonstration Program	7/25/2008
USCIS	Fraud Detection and National Security Data System	7/30/2008
TSA	Screening of Passengers by Observation Techniques	8/5/2008
USCIS	Customer Identity Verification Project	8/14/2008
USCIS	United States Citizenship and Immigration Services Person Centric Query Service Update National Security and Records Verification Directorate/Verification Division update	8/14/2008
DHS Wide	HR Solutions	8/14/2008
USCIS	Secure Information Management Service Pilot Update	8/15/2008
ICE	Bond Management Information System Web version	8/18/2008
USCIS	Computer Linked Application Information Management System 4	9/5/2008
USCIS	USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum	9/5/2008
FEMA	Document Management and Records Tracking System	9/10/2008
USCIS	Microfilm Digitization Access System	9/12/2008
Ethics	Financial Disclosure Management program	10/1/2008
S&T	Keeping Schools Safe	10/2/2008
ICE	Data Analysis and Research for Trade Transparency System	10/10/2008
TSA	Secure Flight Program	10/21/2008
USCIS	Alien Change of Address Card (AR-11)	10/21/2008
US-VISIT	First Phase of the Initial Operating Capability (IOC) of Interoperability between the U.S. Department of Homeland Security and the U.S. Department of Justice	10/23/2008
S&T	Reality Mobile Kentucky Project	10/24/2008
NPPD	Chemical Security Awareness Training Update 2	10/27/2008
USCG	Homeport Update	10/27/2008
FEMA	Homeland Security Virtual Technical Assistance Center	11/5/2008
USCIS	PCQ Visa Benefit Adjudicators, Visa Fraud Officers, and Counselor Officers of the Department of State, Bureau of Counselor Affairs	11/6/2008
TSA	Air Cargo Update	11/12/2008
ICE	Law Enforcement Intelligence Fusion System	11/17/2008
CBP	Advance Passenger Information System 2008 update	11/17/2008

Component	Name of System	Date Approved
USCG	Notices of Arrival and Departure Ship Arrival Notification System	11/20/2008
USCIS	Verification Information System 1.4	11/20/2008
OPs	Suspicious Activity Reports Project	11/21/2008
FEMA	NFIP IT	11/25/2008
CBP	Automated Commercial System/ Automated Commercial Environment-Importer Security Filing Data	12/2/2008
CBP	Automated Targeting System update	12/2/2008
USCIS	Customer Relationship Interface System	12/5/2008
CBP	Advanced Passenger Information System - Northern Border Railroad	12/11/2008
IA	Department of Homeland Security State, Local, and Regional Fusion Center Initiative	12/11/2008
S&T	Future Attribute Screening Technology Mobile Modular	12/11/2008
USCIS	Scheduling and Notification of Applicants for Processing	12/16/2008
USSS	CPNI Reporting	12/17/2008
USCIS	Changes to Requirements Affecting H-2A Nonimmigrant's and Changes to Requirements Affecting H-2B Nonimmigrant's and Employers Final Rules	12/19/2008
TSA	Stand-Off Detection	12/23/2008
FEMA	Disaster Assistance Improvement Program	12/30/2008
DHS Wide	Directory Services and Email System	1/14/2009
USCIS	Correspondence Handling and Management Planning System	1/14/2009
US-VISIT	US VISIT Additional Aliens	2/10/2009
TSA	Maryland 3	2/20/2009
S&T	FireGround Compass	4/9/2009
DHS Wide	HSPD-12 Personal Identity Verification Management System Update	4/10/2009
S&T	Security and Video Quality for the Public Safety Statement of Requirements Project	4/10/2009
USCIS	Compliance Tracking and Management System	4/30/2009
US-VISIT	US VISIT Exit PIA update	5/21/2009
USCG	Vessel Requirements for Notices of Arrival and Departure and Automatic Identification System to add the Notice of Arrival on the Outer Continental Shelf	6/4/2009
DHS Wide	PRISM	6/4/2009
NPPD	Chemical Facility Anti-Terrorism Standards Update	6/5/2009
NPPD	Chemical Facility Anti-Terrorism Standards Chemical Facility Management System (CHEMS)	6/15/2009
DHS Wide	DHS Wide Portals	6/15/2009
USCG	National Pollution Funds Center	6/18/2009

C. Published SORNs

The table below lists all SORNs published in the Federal Register between July 1, 2008 and June 30, 2009.

Component	Name of System	Date Published in the Federal Register
CBP	**DHS/CBP-007**, Border Crossing Information	7/25/2008
CBP	**DHS/CBP-008**, Non Federal Entities Data System (NEDS)	7/25/2008
ICE	**DHS/ICE-002,** ICE Pattern Analysis and Information Collection (ICEPIC)	8/18/2008
USCIS	**DHS/USCIS-006** Fraud Detection and National Security Data System (FDNS DS)	8/18/2008
ICE	**DHS/ICE-004**, Bond Management Information System (BMIS)	9/11/2008
USCIS	**DHS/USCIS-007** USCIS Benefits Information System	9/29/2008
USCG	**DHS/USCG-062,** Law Enforcement Intelligence Database (73 FR 28135)	9/30/2008
DHS	**DHS/All 009** Department of Homeland Security Advisory Committees	10/3/2008
DHS	**DHS/All 012** Department of Homeland Security Childcare	10/3/2008
USCG	**DHS/USCG-024,** United States Coast Guard Auxiliary Database	10/7/2008
DHS	**DHS/All 007** Department of Homeland Security Accounts Payable	10/17/2008
DHS	**DHS/All 008** Department of Homeland Security Accounts Receivable	10/17/2008
DHS	**DHS/All 014** Department of Homeland Security Emergency Personnel Location Records	10/17/2008
DHS	**DHS/All 018** Department of Homeland Security Grievances, Appeals, and Disciplinary Action Records	10/17/2008
DHS	**DHS/All 010** Department of Homeland Security Asset Management Records	10/23/2008
DHS	**DHS/All 017** Department of Homeland Security General Legal Records	10/23/2008
DHS	**DHS/All 019** Department of Homeland Security Payroll, Personnel, and Time and Attendance Records	10/23/2008
DHS	**DHS/All 021** Department of Homeland Security Contractors and Consultants	10/23/2008
DHS	**DHS/All 013** Department of Homeland Security Claims Records	10/28/2008
DHS	**DHS/All 015** Department of Homeland Security Employee Assistance Program Records	10/31/2008
DHS	**DHS/All 022** Department of Homeland Security Drug Free Workplace Records	10/31/2008
ICE	**DHS/ICE-005**, Trade Transparency Analysis and Research (TTAR)	10/31/2008
USCG	**DHS/USCG-002,** United States Coast Guard Employee Assistance Program Records	10/31/2008
USCG	**DHS/USCG-008,** United States Coast Guard Courts Martial Case Files	10/31/2008
DHS	**DHS/All -011** Department of Homeland Security Biographies and Awards	11/10/2008
DHS	**DHS/All 016** Department of Homeland Security Correspondence Records	11/10/2008
DHS	**DHS/All 020** Department of Homeland Security Internal Affairs	11/14/2008
CBP	**DHS/CBP-005**, Advanced Passenger Information (APIS) (72 FR 48349)	11/18/2008
DHS	**DHS/All 002 -** DHS Mailing and Other Lists System (69 FR 70460)	11/25/2008
DHS	**DHS/All 003 -** Department of Homeland Security General Training Records (71 FR 26767)	11/25/2008
DHS	**DHS/All 006** Department of Homeland Security Accident Records	11/25/2008
ICE	**DHS/ICE-006** ICE Intelligence Records System (IIRS)	12/9/2008
ICE	**DHS/ICE-007** Immigration and Customs Enforcement Law Enforcement Support Center Alien Criminal Response Information management System (LESC/ACRIMe)	12/9/2008
ICE	**DHS/ICE-008** Immigration and Customs Enforcement Search, Arrest, and Seizure Records	12/9/2008

Component	Name of System	Date Published in the Federal Register
ICE	**DHS/ICE-010** Immigration and Customs Enforcement Confidential and Other Sources of Information (COSI)	12/9/2008
S&T	**DHS/S&T-001** Science & Technology Directorate Research, Development, Test, and Evaluation Records.	12/9/2008
ICE	**DHS/ICE-009** Immigration and Customs Enforcement External Investigations	12/11/2008
S&T	**DHS/S&T-002** Science & Technology Directorate Personnel Radiation Exposure Records	12/11/2008
USCG	**DHS/USCG-007,** United States Coast Guard Exceptional Family Member Program Records	12/11/2008
USCG	**DHS/USCG-015,** United States Coast Guard Legal Assistance Case Files	12/11/2008
USCG	**DHS/USCG-029,** Notice of Arrival and Departure Information (NOAD)	12/11/2008
USCIS	**DHS/USCIS-004** Verification Information System (72 FR 17569) (73 FR 10793)	12/11/2008
CBP	**DHS/CBP-009** U.S. Customs and Border Protection Nonimmigrant Information System	12/19/2008
CBP	**DHS/CBP-010** U.S. Customs and Border Protection Persons Engage in International Trade in Customs and Border Protection Licensed/Regulated Activities	12/19/2008
CBP	**DHS/CBP-011** TECS	12/19/2008
CBP	**DHS/CBP-012** U.S. Customs and Border Protection Closed Circuit Televisions Systems	12/19/2008
CBP	**DHS/CBP-013** U.S. Customs and Border Protection Seized Assets and Case Tracking System	12/19/2008
CBP	**DHS/CBP-014** Customs and Border Protection Regulatory Audit Archive System (RAAS)	12/19/2008
CBP	**DHS/CBP-015** U.S. Customs and Border Protection Automated Commercial System	12/19/2008
FEMA	**DHS/FEMA-003** Federal Emergency Management Agency National Flood Insurance Program Files	12/19/2008
FEMA	**DHS/FEMA-005** Federal Emergency Management Agency Temporary and Permanent Relocation and Personal and Real Property Acquisitions and Relocation Files	12/19/2008
FEMA	**DHS/FEMA-006** Federal Emergency Management Agency Citizen Corps Database	12/19/2008
FEMA	**DHS/FEMA-007** Federal Emergency Management Agency National Flood Insurance Program Marketing Files	12/19/2008
USCG	**DHS/USCG-006,** United States Coast Guard Great Lakes Registered Pilot and Applicant Pilot Eligibility	12/19/2008
USCG	**DHS/USCG-010,** United States Coast Guard Physical Disability Evaluation System Files	12/19/2008
USCG	**DHS/USCG-011,** United States Coast Guard Military Personnel Health Records	12/19/2008
USCG	**DHS/USCG-012,** United States Coast Guard Request for Remission of Indebtedness	12/19/2008
USCG	**DHS/USCG-014,** United States Coast Guard Military Pay and Personnel	12/19/2008
USCG	**DHS/USCG-016,** United States Coast Guard Adjudication and Settlement of Claims	12/19/2008
USCG	**DHS/USCG-017,** United States Coast Guard Federal Medical Care Recovery Act	12/19/2008
USCG	**DHS/USCG-018,** United States Coast Guard Exchange System and Morale Well-Being and Recreation System Files	12/19/2008
USCG	**DHS/USCG-019,** United States Coast Guard Non-Federal Invoice Processing	12/19/2008
USCG	**DHS/USCG-020,** United States Coast Guard Substance Abuse Prevention and Treatment Program	12/19/2008

Component	Name of System	Date Published in the Federal Register
USCG	**DHS/USCG-021,** United States Coast Guard Appointment of Trustee or Guardian for Mentally Incompetent Personnel Files	12/19/2008
USCG	**DHS/USCG-027,** United States Coast Guard Recruiting Files	12/19/2008
USCG	**DHS/USCG-028,** United States Coast Guard Family Advocacy Case Records	12/19/2008
USCIS	**DHS/USCIS-008** United States Citizenship and Immigration Services Refugee Access Verification Unit	12/19/2008
USSS	**DHS/USSS-001,** United States Secret Service Criminal Investigation Information	12/19/2008
USSS	**DHS/USSS-003,** United States Secret Service Non-Criminal Investigation Information System	12/19/2008
USSS	**DHS/USSS-004,** United States Secret Service Protection Information System	12/19/2008
FEMA	**DHS/FEMA/GOVT-001** National Defense Executive Reserve	1/7/2009
DHS	**DHS/All 023** Personnel Security Management	1/16/2009
DHS	**DHS/All 024** Facility and Perimeter Access Control and Visitor Management	1/16/2009
DHS	**DHS/All 025** Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Department of Homeland Security	1/16/2009
ICE	**DHS/ICE-011** Immigration and Customs Enforcement Removable Alien Records	1/30/2009
USCIS	**DHS/USCIS-009** United States Citizenship Immigration Services Compliance Tracking and Monitoring System	5/22/2009
DHS	**DHS/ALL 026** Personal Identity Verification Management System (71 FR 53697)	6/25/2009
USCG	**DHS/USCG-013,** United States Coast Guard Marine Information for Safety and Law Enforcement (MISLE)	6/25/2009
USCG	**DHS/UCCG-030,** United States Coast Guard Merchant Seamen's Records	6/25/2009

D. S&T Research Principles

Principles for Implementing Privacy Protections in Research Projects
Science and Technology Directorate
United States Department of Homeland Security

INTRODUCTION

The Department of Homeland Security's (DHS) Privacy Office and Directorate of Science and Technology (S&T) have developed these Principles to provide a privacy-protective framework for conducting critical homeland security research and development. The Privacy Office operates under the direction of the Chief Privacy Officer, who is appointed by and reports directly to the Secretary of the Department. The Office serves to implement section 222 of the Homeland Security Act of 2002,[109] and has programmatic responsibilities involving the Privacy Act of 1974,[110] the Freedom of Information Act ("FOIA"),[111] the privacy provisions of the E-Government Act of 2002,[112] and DHS policies that protect individual privacy associated with the collection, use, and disclosure of PII.[113] Section 222 of the Homeland Security Act of 2002 calls on the Chief Privacy Officer to assume primary responsibility for privacy policy within the Department, and, among other things, to "[assure] that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information."[114]

S&T is the Department's primary research and development arm. S&T organizes the scientific and technological resources of the United States to prevent or mitigate the effects of catastrophic terrorism against the United States or its allies. It both conducts its own research and works in partnership with the private sector and other government agencies to encourage innovation in homeland security research and technology development. S&T research encompasses a wide range of activities, from biological research on animal diseases, to social-behavioral research on the motivations for terrorism, to the development of new physical screening technologies. Many

S&T research projects do not involve or impact PII; however, when PII is involved, S&T works closely with the Privacy Office to ensure that all privacy-sensitive S&T Projects safeguard PII and protect the privacy of individuals.

The Principles set forth below are intended to ensure that S&T builds privacy protections into the design and implementation of its research and development projects in a manner that supports the Department's mission. These principles govern research performed at S&T laboratories, S&T-sponsored research conducted in cooperation with other Federal Government entities, and

[109] Section 222 of the Homeland Security Act of 2002, as amended by section 8305 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (December 17, 2004), 6 U.S.C. § 142.
[110] 5 U.S.C. § 552a.
[111] 5 U.S.C. § 552.
[112] Pub. L. 107-347, 116 STAT. 2899, § 208; 44 U.S.C. Chapter 36.
[113] "Personally identifiable information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, a Legal Permanent Resident, or a visitor to the U.S.
[114] 6 U.S.C. §142(a) (1).

research conducted by external performers under a contract with S&T (collectively referred to as "Projects"). These principles apply specifically to privacy-sensitive projects.

The Privacy Office and S&T will work together to create an implementation plan setting forth general guidance regarding the application of these Principles to new S&T Projects. In addition, the Privacy Office will continue its current practice of assessing each S&T Project through a Privacy Threshold Analysis (PTA). The PTA provides a mechanism for determining whether a given Project is privacy-sensitive, and/or involves or impacts personally identifiable information (PII), and whether a Privacy Impact Assessment (PIA) will be required under the E-Government Act of 2002. During the PTA process, the Privacy Office and S&T will jointly determine and document how best to apply these Principles to each S&T Project.

PRINCIPLES

- **Privacy Assessment Principle:** An assessment of privacy impacts will be integral to the development and implementation of any research project.
  - The Privacy Office will assist S&T in identifying privacy impacts to address in project design and implementation, to ensure that research projects sustain privacy protections relating to the use, collection, and disclosure of PII pursuant to section 222(a)(1) of the Homeland Security Act. An appropriately cleared S&T or external expert will participate in the privacy assessment to explain scientific aspects of a proposed research project where a deeper understanding is needed to make decisions regarding the use of PII.
  - All projects will complete a Privacy Threshold Analysis (PTA). Privacy Office staff and the S&T Privacy Officer will review each PTA to determine how best to apply these Principles to each project.
- **Purpose Specification Principle:** A project's purpose will be clearly articulated and documented through an internal/external project review process.
  - **Legal Authorization:** Projects will be structured to function consistent with all relevant legal requirements.
  - **Purpose Limitation:** Projects will only engage in research that is within the scope of their documented purpose(s).
  - **Effectiveness Reviews:** Projects determined by the Chief Privacy Officer to be privacy-sensitive will include an initial review before commencement of research involving PII. The review will be both internal (by S&T staff other than the project's proponents) and external (by experts with appropriate security clearances), and will assess the project's likely effectiveness in accomplishing the documented purpose(s).
- **Data Quality and Integrity Principle:** Projects will endeavour to only use PII that is reasonably considered accurate and appropriate for their documented purpose(s), and to protect the integrity of the data.
  - Projects will exercise due diligence in evaluating the accuracy and relevance of any publicly-available or commercially-available data used, to ensure the research effort's soundness and the integrity of the research results.

- **Data Minimization Principle:** Projects will use the least amount of PII consistent with their documented purpose(s), and will use PII minimization techniques such as synthetic data or anonymization where appropriate and practicable.
- **Use Limitation Principle:** Projects will use PII consistent with all applicable System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), and other privacy notices and policies, regardless of the source of the data (i.e., whether the data is collected directly by the Department of Homeland Security or its contractors, or is obtained by the Department or its contractors from third-party sources).
- **Data Security Principle:** Projects will take all reasonable steps necessary to maintain the security of the PII they use, and to protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.
- **Audit Principle:** Projects involving PII will employ automated and/or non-automated auditing procedures, as appropriate, to ensure compliance with project access and data usage rules ("rules" are specific instructions implementing an applicable project policy, notice, and/or legal requirement).
- **Transparency Principle:** Projects involving PII will foster public trust by publishing PIAs and other public notices, except where the research is classified or Law Enforcement Sensitive (LES). PIAs will be conducted for classified or LES research projects, and when possible, a redacted version will be published.
- **Redress Principle:** The Privacy Office, in conjunction with S&T's Privacy Officer, will develop and administer a redress program to handle inquiries and complaints regarding any S&T research projects involving PII.
- **Training Principle:** The Privacy office, in conjunction with S&T's Privacy Officer, will provide privacy training for all project personnel regarding DHS privacy policy and any privacy protections specific to a particular project.

E. Acronym List

Acronym List	
ABA	American Bar Association
ACLU	American Civil Liberties Union
ADIS	Arrival and Departure Information System
AILA	American Immigration Lawyers Association
ANSI	American National Standards Institute
APEC	Asia Pacific Economic Cooperation
ASAP	American Society of Access Professionals
ATS	Automated Targeting System
BCI	Border Crossing Information
BDO	Behavior Detection Officer
C&A	Certification and Accreditation
CBP	U.S. Customs and Boarder Protection
CCTV	Closed Circuit Television
CDT	Center for Democracy & Technology
CFAA	Computer Fraud and Abuse Act
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIPP/G	Certified Information Privacy Professional/Government
CISO	Office of the Chief Information Security Officer
CLIA	Civil Liberties Impact Assessment
CONOPS	Continuity of Operations
CNCI	Comprehensive National Cybersecurity Initiative
CRCL	Civil Rights and Civil Liberties
CRE	Computer-Readable Extract
CS&C	Office of Cybersecurity and Communications
CSO	Chief Security Officer
DAA	Designated Approving Authority
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	Department of Homeland Security
DIB	Data Integrity Board
DOJ	Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
EAB	Enterprise Architecture Board
EACOE	Enterprise Architecture Center for Excellence
EDL	Enhanced Drivers License
E-Gov	E-Government Act of 2002
EOC	Enterprise Operations Center
ESTA	Electronic System for Travel Authorization
EU	European Union
FACA	Federal Advisory Committee Act
FAR	Federal Acquisition Regulation
FDNS-DS	Fraud Detection and National Security Data System
FEMA	Federal Emergency Management Agency
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FOC	Full Operational Capability

Acronym List	
FOIA	Freedom of Information Act
FR	Federal Register
FTC	Federal Trade Commission
FTE	Full Time Employee
FTS	Fraud Tracking System
FY	Fiscal Year
GAO	Government Accountability Office
HLCG	High Level Contact Group
HSA	Homeland Security Act
I&A	Office of Intelligence and Analysis
IA	Information Assurance
IAFIS	Integrated Automated Fingerprint Identification System
IAPP	International Association of Privacy Professionals
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICE	U.S. Immigration and Customs Enforcement
ICO	Information Commissioner's Office
IDENT	Automated Biometric Identification System
IdM sub-IPT	Identity Management sub-Integrated Product Team
IOC	Initial Operational Capability
IPP	International Privacy Policy
IPT	Integrated Project Team
IRTPA	The Intelligence Reform and Terrorism Prevention Act of 2004
ISAA	Information Sharing Access Agreement
ISCC	Information Sharing Coordination Council
ISE	Information Sharing Environment
ISGB	Information Sharing Governance Board
ISO	International Organization for Standardization
ISSM	Information System Security Manager
ISSO	Information Systems Security Officers
IT	Information Technology
ITLMS	Information Technology Life Cycle Management System
LES	Law Enforcement Sensitive
LESC/ACRIMe	Law Enforcement Support Center Alien Criminal Response Information Management System
LPR	Legal Permanent Resident
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCSD	National Cybersecurity Division
NEDS	Non-Federal Entity Data System
NIISO	National Immigration Information Sharing Operation
NOA	Notice of Arrival
NOAD	Notice of Arrival and Departure Information
NOD	Notice of Departure
NPPD	National Protection and Programs Directorate
NPRM	Notice of Proposed Rule Making
OECD	Organization for Economic Cooperation and Development
OIA	Office of International Affairs
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPEN	Openness Promotes Efficiency in our National Government Act of 2007

Acronym List	
ISGB	Information Sharing Governance Board
PCSC	Preventing and Combating Serious Crime
PGC	Privacy Guidelines Committee
PIA	Privacy Impact Assessment
PIHG	Privacy Incident Handling Guide
PII	Personally Identifiable Information
PM–ISE	Program Manager for the Information Sharing Environment
PNR	Passenger Name Record
PPOC	Privacy Point of Contact
Privacy Act	Privacy Act of 1974
PTA	Privacy Threshold Analysis
RAAS	Regulatory Audit Archive System
RFID	Radio Frequency Identification
S&T	Science and Technology Directorate
SAR	Suspicious Activities Reporting
SBInet	Secure Border Initiative
SCO	Screening Coordination Office
SES	Senior Executive Service
SLWG	State and Local Working Group
SMC	Shared Mission Community
SMRWG	Social Media Roundtable Working Group
SOP	Standard Operating Procedures
SORN	System of Record Notice
SPOT	Screening of Passengers by Observation Techniques
SSA	Social Security Administration
SSN	Social Security Number
State	Department of State
TECS	Treasury Enforcement Communication System
TIC	Trusted Internet Connection
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
UK	United Kingdom
US-CERT	U.S. Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	U.S. Secret Service
VWP	Visa Waiver Program
WG	Working Group
WHTI	Western Hemisphere Travel Initiative
WPISP	Working Party on Information and Privacy