Privacy Office

Fourth Quarter Fiscal Year 2011 Report to Congress

Department of Homeland Security Report of the Chief Privacy Officer Pursuant to Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*

November 22, 2011

Homeland Security

I. FOREWORD

November 22, 2011

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *Fourth Quarter Fiscal Year 2011 Report to Congress*. This quarterly report includes activities from June 1, 2011 – August 31, 2011.

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[1] requires the DHS Privacy Office to report quarterly on the:

- Number and types of privacy reviews of Department actions undertaken;
- Type of advice provided and the response given to such advice;
- Number and nature of privacy complaints received by DHS for alleged violations along with a summary of the disposition of such complaints; and
- Privacy training and awareness activities conducted by the Department to help reduce privacy incidents and increase adoption of our privacy risk management framework.

The DHS Office for Civil Rights and Civil Liberties will provide a separate report regarding civil liberties.

The DHS Chief Privacy Officer is the first statutorily-mandated Chief Privacy Officer in the Federal Government. The DHS Privacy Office is founded upon the responsibilities set forth in Section 222 of the *Homeland Security Act of 2002* ("Homeland Security Act") as amended.[2] The mission of the DHS Privacy Office is to sustain privacy protections and to promote transparency of government operations while achieving the mission of the Department. Within DHS, the Chief Privacy Officer implements Section 222 of the Homeland Security Act,[3] the *Privacy Act of 1974*,[4] the *Freedom of Information Act*[5] (FOIA), the *E-Government Act of 2002*,[6] and the numerous laws, executive orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personally identifiable information (PII) collected, used, maintained, or disseminated by DHS.

---

[1] 42 U.S.C. § 2000ee-1(f)
[2] 6 U.S.C. § 142
[3] 6 U.S.C. § 142
[4] 5 U.S.C. § 552a *et seq.*, as amended.
[5] 5 U.S.C. § 552
[6] Pub. L. 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 101 note.]

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Joseph R. Biden
President, United States Senate

The Honorable John Boehner
Speaker, U.S. House of Representatives

The Honorable Joseph I. Lieberman
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Charles Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Dianne Feinstein
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Saxby Chambliss
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Peter T. King
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Darrell Issa
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Lamar Smith
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Mike Rogers
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable C. A. Dutch Ruppersberger
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Inquiries about this report may be directed to the DHS Privacy Office at 703-235-0780 or privacy@dhs.gov. This report and other information about the Office are available at www.dhs.gov/privacy.

Sincerely,

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security

DHS PRIVACY OFFICE
FOURTH QUARTER FY 2011
SECTION 803 REPORT TO CONGRESS

Table of Contents

II. LEGISLATIVE LANGUAGE

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, 42 U.S.C. § 2000ee-1, includes the following requirement:

> (f) Periodic Reports-
>
> (1) IN GENERAL- The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than quarterly, submit a report on the activities of such officers--
>
> (A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;
>
> (ii) to the head of such department, agency, or element; and
>
> (iii) to the Privacy and Civil Liberties Oversight Board; and
>
> (B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.
>
> (2) CONTENTS- Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including--
>
> (A) information on the number and types of reviews undertaken;
>
> (B) the type of advice provided and the response given to such advice;
>
> (C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and
>
> (D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

III. PRIVACY REVIEWS

The DHS Privacy Office reviews information technology (IT) systems and programs that may have a privacy impact. For purposes of Section 803 reporting, reviews include the following activities:

1. Privacy Threshold Analyses (PTA) – The DHS foundational mechanism for reviewing IT systems, programs, and other activities for privacy protection issues to determine whether a more comprehensive analysis is necessary through the Privacy Impact Assessment process;
2. Privacy Impact Assessments (PIA) required under the *E-Government Act of 2002*, the *Homeland Security Act of 2002*, as amended, by policy or other law;
3. Systems of Records Notices (SORN) and associated Privacy Act Exemptions as required under the *Privacy Act*;
4. Privacy Act Statements as required under Section (e)(3) of the Privacy Act to provide notice to individuals at the point of collection;
5. Computer Matching Agreements;
6. Data Mining Report as defined by Congress under Section 804 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*; and
7. Privacy reviews of IT and program budget requests, including OMB 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board.

Q4 FY2011 Reviews	
Review Type	**# of Reviews**
Privacy Threshold Analyses	167
Privacy Impact Assessments	29
System of Records Notices and Associated Privacy Act Exemptions	6
Privacy Act (e)(3) Statements	15
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Reviews of IT and Program Budget Requests	83
Total Reviews	***300***

Privacy Impact Assessments
The PIA process is one of the key mechanisms used to assure that the Department's use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information. As of August 31, 2011, 80 percent of the Department's Federal Information Security Management Act (FISMA) systems that require a PIA are currently covered by a PIA, an increase from 76 percent at the end of the third quarter. Additionally, the Department has implemented a triennial review program for legacy PIAs to assess and confirm that these systems are still operating within the originally published parameters. As these systems are renewed, notification will be added to the previously published PIA to inform the public that a review has been conducted for that system. A complete list of PIAs conducted by DHS can be found on our website. The following are eight examples of the 29 PIAs published during this reporting period. *Please note that any update to an existing PIA is listed with a small letter after the number, which refers to the original PIA number.*

DHS/CBP/PIA-009(a), TECS System: Customs and Border Protection Primary and Secondary Processing (TECS) National Suspicious Activity Report (SAR) Initiative –
Background: Customs and Border Protection (CBP) published this update to its 2010 PIA. TECS (not an acronym) is the updated and modified version of the former Treasury Enforcement Communications System. TECS is owned and managed by CBP. TECS is the principal system used by officers at the border to assist with screening and determinations regarding admissibility of arriving persons.
Purpose: This update evaluates the privacy impacts of identifying certain of the operational records maintained in TECS as SARs for inclusion in the National SAR Initiative, which is led by the Department of Justice on behalf of the entire Federal Government. *(August 5, 2011)*

DHS/NPPD/PIA-017(a), National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative Update –
Background: The National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) National Infrastructure Coordinating Center (NICC) published this PIA update to reflect activities under its SAR Initiative. The NICC SAR Initiative serves as a mechanism by which a report involving suspicious behavior related to an observed encounter or reported activity is received and evaluated to determine its potential nexus to terrorism.
Purpose: NICC is conducting this PIA update because SARs occasionally contain PII, and NICC will be collecting and contributing SAR data for reporting and evaluation proceedings. DHS is updating this PIA to clarify that redacted NICC Patriot Reports are reports that have been scrubbed of any identifiable information, to include business information as well as PII. *(August 12, 2011)*

DHS/TSA/PIA-016(a), Screening of Passengers by Observation Techniques Program –
Background: The Screening of Passengers by Observation Techniques (SPOT) program is a behavior observation and analysis program designed to provide the Transportation Security Administration (TSA) Behavior Detection Officers (BDOs) with a means of identifying persons who pose or may pose potential transportation security risks by focusing on behavioral criteria indicative of criminal or terrorist activitiy. The SPOT program is a derivative of other behavioral analysis programs that have been successfully employed by law enforcement and security personnel both in the U.S. and around the world.
Purpose: This PIA update reflects that TSA will pilot the use of BDOs as part of the security checkpoint process, by incorporating BDO interaction with passengers. *(August 5, 2011)*

DHS/USCIS/PIA-027(a), Refugees, Asylum, and Parole System and the Asylum Pre-Screening System Update –

Background: U. S. Citizenship and Immigration Services (USCIS) updated the PIA for the Refugees, Asylum, and Parole System (RAPS), and the Asylum Pre-Screening System (APSS) in order to provide further notice of the expansion of the routine sharing of RAPS information with the intelligence community in support of the Department's mission to protect the United States from potential terrorist activities.

Purpose: DHS has entered into an MOU with NCTC in order to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks, and coincides with a recent exercise of the Secretarial disclosure authority under 8 CFR §208.6(a). DHS and NCTC have placed specific safeguards in this MOU to ensure that the data is used appropriately and in accordance with the existing system of records notice for Asylum Information and Pre-Screening (last published January 5, 2010 at 75 FR 409) and this PIA. *(June 30, 2011)*

DHS/TSA/PIA-018(b), Secure Flight Program Update –

Background: The Secure Flight program matches identifying information of aviation passengers, and certain non-travelers granted access to an airports sterile area, against the No Fly and Selectee portions of the consolidated and integrated terrorist watch list and, if warranted by security considerations, other watch lists maintained by the Federal Government. The Transportation Security Administration (TSA) published a Final Rule and PIA in October 2008 outlining TSA's expected implementation of the Secure Flight program.

Purpose: This update reflects changes in the Secure Flight operational environment. Unless otherwise noted, the information provided in previously published PIAs remains in effect. *(August 15, 2011)*

DHS/ALL/PIA-027(a), Watchlist Update –

Background: DHS currently uses the Terrorist Screening Database (TSDB), a consolidated database maintained by the Department of Justice Federal Bureau of Investigation Terrorist Screening Center (TSC) that contains identifying information about those known or reasonably suspected of being involved in terrorist activity, in order to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. In July 2010, DHS launched an improved method of transmitting TSDB data from TSC to DHS through a new service called the "DHS Watchlist Service" (WLS). At that time, DHS published a PIA to describe and analyze privacy risks associated with this new service. The WLS maintains a synchronized copy of the TSDB, which contains PII, and disseminates the TSDB data to authorized DHS Components. The WLS does not alter DHS's authority or use of the TSDB.

Purpose: DHS issued this PIA update to add CBP's Automated Targeting System as an authorized recipient of TSDB data via the WLS. *(July 19, 2011)*

DHS/CBP/PIA-007(a), Electronic System for Travel Authorization Fee and Information Sharing Update –

Background: CBP published this update to the PIA for the Electronic System for Travel Authorization (ESTA) Fee and Information Sharing dated June 3, 2008. ESTA is a web-based application and screening system used to determine whether certain aliens are eligible to travel to the United States under the Visa Waiver Program.

Purpose: This update evaluates the privacy impacts of updating the login procedures, collecting an application fee, and adding the Pay.gov tracking number and country of birth information to the ESTA System of Records. Additionally, this update provides further notice of the expansion of routine

sharing of ESTA with the intelligence community in support of the Department's mission to protect the United States from potential terrorist activities. *(July 18, 2011)*

DHS/NPPD/PIA-019, Ammonium Nitrate Security Program –
Background: NPPD published this PIA to provide a comprehensive analysis of the proposed Ammonium Nitrate Security Program, which seeks to prevent the misappropriation or use of ammonium nitrate in an act of terrorism by regulating the sale and transfer of ammonium nitrate by ammonium nitrate facilities.
Purpose: This PIA provides transparency into how the proposed Ammonium Nitrate Security Program will support the homeland security and infrastructure protection missions of NPPD through the collection of PII, and describes reasonable mitigation solutions to address privacy and security risks.

Note: This PIA is made available concurrently with the Department's publication in the Federal Register of a Notice of Proposed Rulemaking for the Ammonium Nitrate Security Program, see 76 FR 46908 (August 3, 2011). This PIA will be updated with any changes to the program concurrently with the rulemaking process. *(July 25, 2011)*

System of Records Notices
In addition to the PIAs published during this reporting period, DHS also published six Privacy Act SORNs to support systems at the Department. As of August 31, 2011, 95 percent of the Department's FISMA systems that require a SORN are currently covered by an applicable SORN. SORNs continue to receive biennial reviews to ensure that they conform to and comply with the standards outlined in the Privacy Act; if no update is required, the SORN remains valid. The following are three examples of SORNs that were published during the reporting period and can be found on our website:

- ***DHS/FEMA-001, National Emergency Family Registry and Locator System*** –
  FEMA's NEFRLS System of Records collects information from Law Enforcement Officials (LEOs) for the purpose of responding to a Missing Persons Report. The information is collected from LEOs to facilitate verification of their identity and status as members of law enforcement. The collection of an LEO's identifying information increased the amount of identifying information collected and maintained by the DHS/FEMA-001 NEFRLS System of Records. Information collected is stored on FEMA secured servers and/or in locked cabinets with secured facility access controls. *(August 30, 2011)*

- ***DHS/ALL-030, Use of the Terrorist Screening Database System of Records -***
  The Department maintains a mirror copy of the Department of Justice/Federal Bureau of Investigation-019 Terrorist Screening Records System of Records, August 22, 2007, in order to automate and simplify the current method for transmitting the Terrorist Screening Database (TSDB) to DHS Components. Additionally, the Department issued a Notice of Proposed Rulemaking concurrent with this system of records in the Federal Register. This newly established system will be included in the Department's inventory of records systems. *(July 6, 2011)*

- ***DHS/NPPD-002, Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records -***
  As part of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 C.F.R. Part 27, under this new system of records, the Department will collect information on individuals--facility personnel and unescorted visitors--who have or are seeking access to restricted areas and critical assets at high-risk chemical facilities, and will compare this information to the Terrorist Screening Database, the terrorist watchlist maintained by the Federal Bureau of Investigation's Terrorist Screening Center. The Department issued a Notice of Proposed Rulemaking concurrently with this system of records in the Federal Register to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. This newly established system of records will be included in the DHS inventory of records systems. *(June 14, 2011)*

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

During this reporting period, DHS conducted the following privacy training:

- **52,729** DHS personnel and contractors completed the mandatory computer-assisted privacy training course, *Culture of Privacy Awareness* (note: this is an annual requirement).
- **5,512** DHS personnel attended instructor-led privacy training courses, including privacy training for new employees.

New Employee Training

- The DHS Privacy Office provides introductory privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees. Many of the Component Privacy Offices also offer introductory privacy training for new employees.
- The DHS Privacy Office provides privacy training each month as part of the two-day *DHS 101* training course, which is required for all new and existing headquarters staff.

Fusion Center Training

- The DHS Privacy Office continued to collaborate with the Office of Intelligence and Analysis (I&A) and the Office for Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to staff at state and major urban area fusion centers.
    - During this reporting period, 77 people were trained.
- The DHS Privacy Office also provides training to I&A intelligence professionals selected for assignment to fusion centers, as required under section 511 of the *9/l1 Commission Act*.
    - In August, DHS Privacy Office staff trained 51 analysts on privacy issues entailed in suspicious activity reporting.

Annual Privacy Compliance Workshop

In June 2011, the DHS Privacy Office held a public workshop to provide in-depth training on the DHS privacy compliance process. The two-day workshop covered privacy compliance fundamentals, as well as how to develop and draft a PTA, PIA, and SORN. The workshop also addressed how to request access to records under the Privacy Act, and included hands-on case studies and panels highlighting the latest developments in privacy policy. 258 individuals from many Federal agencies attended.

B. DHS Privacy Office Awareness & Outreach

Publications

During this reporting period, the DHS Privacy Office issued a new Privacy Policy Guidance Memorandum 2011-02 entitled *Roles & Responsibilities for Shared IT Services*. This new policy, signed by the Chief Privacy Officer, the Assistant Secretary for Policy, the Chief Information Officer, and the Director of Publications and Mail Management, establishes policy on DHS Components sharing IT systems and data. This publication can be found on our website, www.dhs.gov/privacy.

Outreach

Both of these educational opportunities are open to all Federal employees and contractors:

- *DHS Privacy Office Speaker Series* – The DHS Privacy Office launched a new series of public workshops for the period July 2011 through April 2012. The featured topic this year is cybersecurity, with outside experts presenting on botnets, online identities, and virtual worlds.
- *Workshop Series Sponsored by the Federal CIO Council Privacy Committee* – As an active member of this committee, the DHS Privacy Office is collaborating with privacy representatives from other Federal agencies to host a series of monthly workshops on current privacy topics.

Meetings & Events

- Center for Democracy & Technology Roundtable – On June 14, the Chief Privacy Officer spoke on *The Emerging Reality of Big Data: Over the Horizon Opportunities and Challenges for National Security and Privacy.*
- 2011 Computers, Freedom, and Privacy Conference – On June 14 and 16, the Chief Privacy Officer participated in two separate panel discussions: *A Clash of Civilizations: The EU and US Negotiate the Future of Privacy*, and *The Privacy Profession – Corporate Apologists, or Agents of Positive Change?*
- Gartner Security & Risk Management Summit – On June 20, the Chief Privacy Officer participated on a panel entitled *The Future of Privacy.*
- Data Privacy and Integrity Advisory Committee (DPIAC) Meeting – On July 11, the DPIAC held a public meeting. The agenda included remarks by the Deputy Secretary on the Department's international information sharing initiatives, a report from the Chief Privacy Officer on Privacy Office activities since the DPIAC's May 2011 meeting, and a briefing by the Senior Privacy Officer for the National Protection and Programs Directorate (NPPD) on the Component's implementation of Department privacy policy.
- Association of Government Accountants 60th Annual Professional Development Conference & Exposition – On July 12, the Chief Privacy Officer participated on the panel entitled *Protecting Data in an Era of Open Government: What WikiLeaks Can Teach Us.*
- Privacy Information for Advocates Meeting – On July 15, the Chief Privacy Officer hosted this quarterly meeting which is designed to proactively engage the privacy community on privacy issues.
- National Strategy for Trusted Identities in Cyberspace Privacy Workshop – On July 26-27, the DHS Privacy Office's Senior Advisor for Information Sharing participated in this workshop, hosted by the National Institute of Standards and Technology. The workshop brought together representatives of industry, government, advocacy groups, and academia to discuss the privacy risks and benefits of online identity management solutions.

C. Component Privacy Office Awareness & Outreach

Office of Intelligence and Analysis Privacy Office

- 12 employees and contractors attended an inaugural in-processing session which included an overview of the I&A SORN, along with select PIAs and the safe handling of PII. This is expected to become a regular event for all newly-assigned employees and contractors.

Transportation Security Administration Privacy Office

- TSA privacy staff participated in comprehensive privacy discussions and workshops at the 2011 Computers, Freedom, and Privacy Conference.
- TSA Privacy Officer served as a presenter at the U.S. Department of Agriculture's Annual Cybersecurity Expo.
- TSA privacy staff provided training to 15 project team members requesting guidance on PII safe handling. They also provided guidance to 20 individuals via phone & the TSAPrivacy@dhs.gov mailbox.
- TSA privacy staff provided hands-on Trusted Agent FISMA, PTA, PIA, and SORN training to 85 Information System Security Officers at a monthly town hall meeting.

U.S. Citizenship and Immigration Services Privacy Office

- USCIS Office of Privacy hosted a mandatory privacy awareness training for all headquarters employees and contractors at the Tomich Conference Center in Washington, D.C. The training was conducted twice a month starting in June through September 2011. Over 350 employees and contractors were trained.
- USCIS privacy staff provided training on how to safeguard PII to USCIS staff at:
    1. The USCIS Contract Management Seminar.
    2. The FDNS Basic Instructor Training.
    3. The USCIS International Operations Overseas Training.

United States Coast Guard Privacy Office

In an effort to heighten privacy awareness throughout the Coast Guard, the Privacy Office sent one representative to the Annual Civil Rights Conference held in San Diego, California. 75 Coast Guard Civil Rights Advisors were in attendance for the one-hour presentation led by the Coast Guard privacy staff which included an interactive discussion on acceptable privacy safeguards to employ in the workplace.

U.S. Immigration & Customs Enforcement Privacy Office

- ICE privacy staff emailed a privacy tip to all employees.
- ICE Privacy Officer presented a privacy overview at ICE's Office of the Principal Legal Advisor Conference on July 19, 2011.

V. PRIVACY COMPLAINTS AND DISPOSITIONS

For purposes of Section 803 reporting, complaints are written allegations of harm or violation of privacy compliance requirements filed with the DHS Privacy Office or DHS Components or programs. The categories of complaints reflected in the following table are aligned with the categories detailed in the Office of Management and Budget's Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. Complaints are received from U.S. citizens, Legal Permanent Residents, visitors, or aliens.[7]

Type of Complaint	Number of complaints received during this reporting period	Disposition of Complaint		
		Closed-Responsive Action Taken*	In-Progress (Current Period)	In-Progress (Prior Periods)
Process & Procedure	6	6	1	1
Redress	0	2	0	0
Operational	289	266	49	7
Referred	17	19	0	0
Total	***312***	***293***	***50***	***8***

*This category may include responsive action taken on a complaint received from a prior reporting period.

Complaints are separated into four categories:

1. ***Process and Procedure****:* Issues concerning process and procedure, such as consent, or appropriate notice at the time of collection.
   Example: An individual submits a complaint that alleges a program violates privacy by collecting Social Security numbers without providing proper notice.
2. ***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.[8]
3. ***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.
4. ***Referred****:* The DHS Component or the DHS Privacy Office determined that the complaint would be more appropriately handled by another Federal agency or entity, and referred the complaint to the appropriate organization. This category does not include referrals within DHS. The referral category both serves as a category of complaints and represents responsive action taken by the Department unless a complaint must first be resolved with the external entity.
   Example: An individual has a question about his or her driver's license or Social Security number, which the DHS Privacy Office refers to the proper agency.

[7] *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.*

[8] This category excludes Freedom of Information Act and Privacy Act requests for access which are reported annually in the Annual FOIA Report. Additionally, this category excludes Privacy Act Amendment requests, which are reported annually in the DHS Privacy Office Annual Report to Congress.

DHS Components and the DHS Privacy Office report disposition of complaints in one of the two following categories:

1. *Closed-Responsive Action Taken*: The DHS Component or the DHS Privacy Office reviewed the complaint and a responsive action was taken. For example, an individual may provide additional information to distinguish himself from another individual. In some cases, acknowledgement of the complaint serves as the responsive action taken. This category may include responsive action taken on a complaint received from a prior reporting period.

2. *In-Progress*: The DHS Component or the DHS Privacy Office is reviewing the complaint to determine the appropriate action and/or response. This category identifies in-progress complaints from both the current and prior reporting periods.

The following are examples of complaints received during this reporting period, along with their disposition:

Transportation Security Administration

Complaint: A TSA employee complained that airport managers invaded her privacy by allowing a fellow employee of the same grade to observe a pre-decisional meeting regarding the employee's dismissal. The complainant alleged that the fellow employee did not have a need to know the information in the performance of his official duties.

Disposition: Following discussions with the facility's leadership, TSA determined that the observing employee, a customer service representative, served as an official witness to the proceedings should a dispute have arisen based on what occurred during the meeting. Therefore, TSA determined that no Privacy Act violation occurred as a result of the witness' presence at the meeting.

U.S. Customs and Border Protection

Complaint: A Lawful Permanent Resident (LPR) contacted the CBP INFO Center regarding repeated secondary referrals upon entry to the U.S. The LPR complained that he had continually been sent to secondary screenings when entering the United States due to an outstanding USCIS record that indicated the LPR had been the subject of a deportation order. The LPR advised that he had obtained a letter from CBP's Admissibility Review Office that stated he should be admissible. In addition, he secured a court order in which the Immigration Judge ruled the deportation order should be overturned. Nevertheless, because the USCIS record had not been updated or removed, he continued to be questioned in secondary at U.S. Ports of Entry.

Disposition: CBP resolved this issue by working with USCIS to amend the record so that it was recorded under archived status, meaning that it is not actively used, and, as a result, the traveler is no longer routinely sent to secondary screening.

U.S. Customs and Border Protection

Complaint: The CBP INFO Center received numerous complaints from importers about PIERS[9] publicly posting their company and vessel manifest data. Occasional complaints were also fielded about PIERS posting of Sensitive PII for privately imported shipments. In each instance, the complainant was advised that while private sector media services are permitted to collect and publish the information pursuant to 19 CFR 103.31(d), importers may request confidentiality of their information, and such requests provide confidentiality for a period of two years.

Disposition: Importers are directed to send their requests for confidential treatment to CBP's Office of International Trade, Privacy Act Policy and Procedures Branch. The principal cause of individuals' complaints about their PII being published by PIERS is from carriers placing PII into publicly disclosable fields (e.g., cargo description, marks & numbers, etc.). CBP has aggressively sought to alleviate this problem by taking the following steps: 1) advising the carrier community via online communications to stop placing PII into publicly disclosable fields; 2) informing the requestor community that confidentiality is available upon request; 3) implementing fast-track handling of such requests from individuals; 4) coordinating with the trade data companies, on a case-by-case basis, to remove an individual's PII when the problem is found; and 5) counseling Other Government Agencies (OGAs), whose employees are deployed abroad, to both take advantage of vessel manifest confidentiality and ensure that their contracts with moving companies contain provisions against placing PII in fields on shipping documents that will become publicly available on manifests.

[9] PIERS is a comprehensive private sector database of import and export information on the cargoes moving through ports in the U.S., Mexico, Latin America, and Asia.