Privacy Office

First 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

March 16, 2011

Homeland Security

I. FOREWORD

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *First Quarter Fiscal Year 2011 Report to Congress*. This quarterly report includes activities from September 1 - November 30, 2010.

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. 110-53, requires the DHS Privacy Office to report quarterly on the:

1. Number and types of privacy reviews of Department actions undertaken;
2. Type of advice provided and the response given to such advice;
3. Number and nature of privacy complaints received by DHS for alleged violations along with a summary of the disposition of such complaints; and
4. 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") [Public Law 107-296; 6 U.S.C. §142], as amended. 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,[1] the *Privacy Act of 1974*,[2] the *Freedom of Information Act* (FOIA),[3] the *E-Government Act of 2002*,[4] 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.

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

[1] 6 U.S.C. § 101 *et seq.*
[2] 5 U.S.C. § 552a *et seq.*, as amended.
[3] 5 U.S.C. § 552
[4] 44 U.S.C. § 3501

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 Jeff Sessions
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 relating to 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
FIRST QUARTER FY 2011
SECTION 803 REPORT TO CONGRESS

II. PRIVACY REVIEWS

The DHS Privacy Office performs a number of different reviews of 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, which 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.

Q1 FY2011 Reviews	
Review Type	**# of Reviews**
Privacy Threshold Analyses	135
Privacy Impact Assessments	14
System of Records Notices and Associated Privacy Act Exemptions	9
Privacy Act (e)(3) Statements	5
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Reviews of IT and Program Budget Requests	0
Total Reviews for Q1 FY11	***163***

Privacy Impact Assessments

At the Department, PIAs represent a substantial effort on the part of Components, Component Privacy Officers, Privacy Points of Contact, and the DHS Privacy Office. The PIA process is one of the key mechanisms used to assure that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information. As will be reflected in the First Quarter FY 2011 Quarterly *Federal Information Security Management Act* (FISMA) report regarding agency privacy management submitted to the Office of Management and Budget, 73 percent of the Department's FISMA systems that require a PIA are currently covered by a PIA. A complete list of PIAs conducted during this reporting period can be found on our website. Below are a few examples:

- *Citizenship Immigration Data Repository* – The DHS U.S Citizenship and Immigration Services (USCIS) developed the Citizenship Immigration Data Repository (CIDR), hosted on DHS classified networks, in order to make information from multiple USCIS benefits administration systems available for querying by authorized USCIS personnel for the following three purposes: (1) vetting USCIS application information for indications of possible immigration fraud and national security concerns; (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion; and (3) responding to requests for information from the DHS Office of Intelligence and Analysis (I&A) and/or the federal intelligence and law enforcement community members that are based on classified criteria.

- *DHS Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Initiative* – DHS I&A, primarily through the State and Local Program Office in coordination with the Office of Operations Coordination and Planning (OPS), is leading the DHS effort to implement the Nationwide Suspicious Activity Reporting Initiative (NSI). The NSI is a key aspect of the federal Information Sharing Environment that Congress created in the *Intelligence Reform and Terrorism Prevention Act of 2004*. The NSI is overseen by the Department of Justice and is designed to support the sharing of information through the ISE about suspicious activities which are defined as "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity [related to terrorism]." I&A and OPS have been jointly coordinating activities throughout DHS to develop a department-level interface with the NSI that will enable DHS to share Suspicious Activity Reporting that meets the ISE-SAR Functional Standard Version 1.5. The ISE-SAR Functional Standard Version 1.5 defines an ISE-SAR as official documentation of observed behavior reasonably indicative of: pre-operational planning related to terrorism or other criminal activity associated with terrorism. DHS conducted this PIA because ISE-SAR may contain personally identifiable information. This PIA describes the coordinated activities of the DHS ISE-SAR Initiative, including the process for DHS component level review, identification, and submission of ISE-SAR to the NSI Shared Space, as well as the technology that DHS developed to support DHS's participation in the NSI.

- *S&T Research Projects Involving Volunteers* – An integral part of the DHS Science and Technology Directorate's (S&T) mission is to conduct research, development, testing, and evaluation (RDT&E) on technologies or topics related to improving homeland security and combating terrorism. Some S&T RDT&E activities use volunteers to test, evaluate, provide feedback, or otherwise collect data on certain research topics, technologies, equipment, and capabilities related to S&T's mission. Volunteer RDT&E activities require the collection of a range of information from volunteers including work experience, biographic data, and images. RDT&E activities will vary in the types and breadth of data elements and information collected from volunteers. S&T conducted this PIA to establish protections for all volunteer S&T RTD&E activities. Volunteer RDT&E activities that are covered are listed in the PIA.

- *DHS-Wide Social Networking Interaction and Applications* – Social networking interactions and applications include a sphere of non-government websites and web-based tools that focuses on connecting users, inside and outside DHS, to engage in dialogue, share information and media, and collaborate. Third parties control and operate these non-governmental websites; however, DHS may use them as alternative channels to provide robust information and engage with the public. The Department may also use these websites to make information and services widely available, while promoting transparency and accountability, as a service for those seeking information about or services from the Department. This PIA analyzes DHS's use of social networking and how these interactions and applications could result in the Department receiving PII. This PIA describes the information DHS may have access to, how it will use the information, what information is retained and shared, and how individuals can gain access to and correct their information. Appendix A of this PIA will serve as a listing, to be updated periodically, of DHS social networking interactions and applications, approved by the Chief Privacy Officer, that follow the requirements and analytical understanding outlined in this PIA.

System of Records Notices

In addition to the PIAs published during this reporting period, DHS also published Privacy Act SORNs to support systems and initiatives such as CIDR and the DHS ISE-SAR Initiative. As reflected in the Fourth Quarter FY 2010 FISMA Report regarding agency privacy management submitted to OMB, 94 percent of the Department's FISMA systems that require a SORN are currently covered by an applicable SORN. Below are a few examples of SORNs that were published during the reporting period and can be found on our website:

- *DHS/USCIS-012, Citizenship Immigration Data Repository System of Records* – DHS/USCIS developed this SORN for records stored in CIDR which include a mirror copy of USCIS's major immigrant and non-immigrant benefits databases combined into a single user interface and presented in an updated, searchable format on the classified network. This system takes existing USCIS data and recompiles them into a system for the following three purposes: (1) vetting USCIS application information for indications of possible immigration fraud and national security concerns; (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion; and (3) to respond to requests for information from the DHS Office of Intelligence and Analysis and/or the federal intelligence and law enforcement community members that are based on classified criteria. Concurrently with the publication of this SORN, DHS issued a Notice of Proposed Rulemaking to exempt this system from certain provisions of the Privacy Act.

- *Suspicious Activity Reporting* - In support of the DHS ISE-SAR Initiative and Component-level SAR activities, DHS published three SORNs including:

  - *DHS/ALL-031, Information Sharing Environment Suspicious Activity Reporting Initiative System of Records* – To support the DHS ISE-SAR Initiative, DHS developed this SORN to allow DHS to compile suspicious activity report data that meet the ISE-SAR Functional Standard Version 1.5 and share these data with authorized participants in the NSI, including other DHS components, federal departments and agencies, state, local, and tribal law enforcement agencies, and the private sector. Concurrently with the publication of this SORN, DHS issued a Notice of Proposed Rulemaking to exempt this system from certain provisions of the Privacy Act.

  - *DHS/OPS-003, Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records* – This system of records will allow the DHS Office of Operations Coordination and Planning, including the National Operations Center, to collect, plan, coordinate, report, analyze, and fuse information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals. Some of the records in this system are in part transferred from the DHS/Information Analysis and Infrastructure Protection – 001 Homeland Security Operations Center Database system of records, April 15, 2005, with the overall intent of narrowing the focus of these records to the specific purpose outlined in this system of records notice. It is the Department's intent, after all records are transferred into this and other system of records, to retire the DHS/Information Analysis and Infrastructure Protection – 001 Homeland Security Operations Center Database system of records. Concurrent with the publication of the DHS/OPS-003 SORN, DHS issued a Notice of Proposed Rulemaking to exempt this system from certain provisions of the Privacy Act.

  - *DHS/NPPD-001, National Infrastructure Coordinating Center Records System of Records* – This system of records will allow DHS's National Protection and Programs Directorate (NPPD) National Infrastructure Coordinating Center, an element of the National Operations Center, to collect, plan, coordinate, report, analyze, and fuse infrastructure information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the National Infrastructure Coordinating Center. Concurrent with the publication of this SORN, DHS issued a Notice of Proposed Rulemaking to exempt this system from certain provisions of the Privacy Act.

III. ADVICE AND RESPONSES

Privacy Training, Awareness and Outreach

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

- 3,390 DHS personnel attended instructor-led privacy training courses (note: this metric captures each time a person attends training.)
- 72,551 DHS personnel and contractors completed the mandatory computer-assisted privacy training course: *Culture of Privacy Awareness* (note: this is an annual requirement).

New Employee Training:

1. The DHS Privacy Office provides introductory privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees. Component Privacy Offices may also offer introductory privacy training for new employees.
2. 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:

1. During this reporting period, the DHS Privacy Office continued to collaborate with the Office for Civil Rights and Civil Liberties to create and deliver privacy and civil liberties training to over 100 staff from 4 fusion centers.
2. The DHS Privacy Office also continued to provide training to intelligence professionals selected for assignment to fusion centers from I&A, as required under section 511 of the *9/l1 Commission Act*.

New Foreign Attaché Training Program*:*

The goal of this new web-conference series is to raise awareness among DHS international attaches and liaisons on U.S. privacy laws and DHS privacy policies in a foreign policy context. The first seminar, *Data Protection, Privacy, PNR [Passenger Name Record] and More*, was attended by 71 people.

First-Ever Freedom of Information Act Training:

On November 30, 2010, the FOIA team held its first annual Department-wide FOIA workshop. The theme for the one-day workshop, *Operationalizing Transparency as One DHS*, embraced the Secretary's commitment to unifying the Department, as well as the Administration's commitment to transparency and openness in government. The event brought together 106 FOIA professionals from across the Department to learn about the distinct functions of each of the Department's FOIA programs, as well as to discuss ways to work collaboratively and to promote transparency to the fullest extent while protecting information that is critical to accomplishing the Department's mission. DHS Deputy Secretary Lute was the keynote speaker.

A. DHS Privacy Office Awareness & Outreach

Staff Awareness:

- DHS Privacy Office Speaker Series:
  - On October 27, the Assistant General Counsel, Privacy and Civil Liberties Unit, from the Federal Bureau of Investigation, gave a presentation on DNA and privacy, covering recent legal decisions about the collection and use of DNA in law enforcement investigations.

Publications:

- The DHS Privacy Office submitted its *2010 Annual Report to Congress* on September 17. The Report demonstrates the Office's leadership in systematizing privacy protections throughout DHS and across the Federal Government.
- On November 16, in Toronto and on November 19, in Washington, DC, the Chief Privacy Officer participated in two press events for the launch of the November issue of the Wilson Center's Canada Institute Publication "One Issue Two Voices." The Chief Privacy Officer and the publication's counterpoint author, Wesley Wark, discussed privacy and security in border management from both countries' viewpoints.

Meetings & Events:

- Privacy Information for Advocates – On September 17, the Chief Privacy Officer hosted the quarterly Privacy Information for Advocates meeting, which is designed to proactively engage the privacy community on privacy issues.
- State Department International Visitor Program on Data Privacy – On September 23, the DHS Privacy Office hosted ten international visitors from Europe to discuss the U.S. privacy framework and DHS privacy protections. In addition to DHS Privacy Office representatives, the visitors met with the Component privacy officers from US-VISIT and the Transportation Security Administration (TSA).
- Advisory Committee Meeting – On September 28, the DHS Data Privacy and Integrity Advisory Committee held its third 2010 quarterly meeting at the U.S. Government Printing Office headquarters in Washington, DC. In addition to an update by the Chief Privacy Officer on DHS Privacy Office activities since the committee's last meeting in May, the committee heard presentations on enhancing accountability in the DHS compliance process, DHS privacy training programs, and U.S. Customs and Border Protection's (CBP) implementation of DHS privacy policy.
- International Association of Privacy Professionals (IAPP) 2010 Conference – On September 30, the Chief Privacy Officer participated in the *Building a Culture of Privacy* panel at the IAPP conference in Baltimore. Several other senior staff members from the DHS Privacy Office were also panelists.
- 32nd International Data Protection and Privacy Commissioners Conference – On October 27, the Chief Privacy Officer delivered a presentation on *The Position and Role of the Chief Privacy Officer* at the International Data Protection and Privacy Commissioners Conference in Jerusalem. Additionally, the Deputy Chief Privacy Officer delivered a presentation on October 28 on *Government Access to Private Sector Data*.
- Passenger Name Record Outreach in Eastern Europe – From October 28-November 4, the Chief Privacy Officer traveled to Lithuania, Latvia, Estonia, and Finland to conduct outreach on the Department's use of PNR. The Chief Privacy Officer met with Ministries of Justice, Interior, and Foreign Affairs.

- 2010 Federal Privacy Summit – On November 1, the Deputy Chief Privacy Officer and five senior staff members of the DHS Privacy Office participated as moderators and/or speakers at the 2010 Federal Privacy Summit. This annual summit, sponsored by the Chief Information Officers Council's Privacy Committee, provides an opportunity to share best practices and to hear leading experts discuss the issues affecting federal privacy professionals today.

Press:

- On November 16, in Toronto and on November 19 in Washington, DC, the Chief Privacy Officer participated in two press events for the launch of the November issue of the Wilson Center's Canada Institute publication "One Issue Two Voices." The Chief Privacy Officer and the publication's counterpoint author, Wesley Wark, discussed privacy and security in border management from both countries' viewpoints.
- *MacLean's Magazine* – As part of the Woodrow Wilson Center's "One Issue, Two Voices," *MacLean's Magazine* featured the Chief Privacy Officer and Wesley Wark, a professor at the University of Toronto, in an article, "Privacy Information Sharing: The search for an Intelligent Border."
- *The Toronto Star* – "Officer Walks Thin Line between Rights, Security; Complaints Soar as Travelers to U.S. Face Increasing Scrutiny," November 17, 2010.
- Lithuanian interview on Passenger Name Records – On November 1, the Chief Privacy Officer visited Lithuania while touring through Baltic countries and Finland. She wanted to inform the institutions of these countries about the PNR system which soon will be negotiated by Washington and Brussels.

B. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency (FEMA)

- FEMA Privacy Office continues to provide classroom privacy training to its 10 regional field offices.

Federal Law Enforcement Training Center (FLETC)

- FLETC Privacy Office conducted area-specific privacy training for Human Capital and Equal Employment Opportunity managers.

U.S. Immigration & Customs Enforcement (ICE)

- Two privacy *Tip of the Week* broadcasts were emailed to all ICE Employees.
- ICE Privacy Office participated in ICE's Cybersecurity Awareness Month, providing details on safeguarding PII, reporting privacy incidents, and the proper disclosure of PII.
- ICE Privacy Office implemented classroom privacy training at the ICE New-Attorney Training and conducted multiple classroom privacy trainings for the Office of Enforcement and Removal Operations, Office of Principal Legal Advisor field offices, and ICE SharePoint collaboration site administrators.

National Protection and Programs Directorate (NPPD)

- On October 28, NPPD Privacy Officer and DHS Privacy Office staff conducted in-person privacy compliance training to 20 Infrastructure Protection employees.
- On November 18, NPPD Privacy Officer conducted general privacy and compliance training to 14 Federal Protective Service field agents.

Science and Technology Directorate (S&T)

- S&T Privacy Office conducted in-person mitigation training for 11 employees on how to protect and process sensitive Personally Identifiable Information.

Transportation Security Administration (TSA)

- TSA Privacy Office:
  - Attended outreach meeting with the American Civil Liberties Union.
  - Attended a meeting with 40 representatives from religious, transgender, and disabilities representatives.
  - Reviewed approximately 30 intelligence products for sensitive privacy information.
  - Gave a presentation on privacy training and awareness best practices to 50 attendees at the 2010 Federal Privacy Summit.

U.S. Coast Guard (USCG)

- In an effort to heighten privacy awareness throughout the Coast Guard, the USCG Privacy Office sent one representative to the annual Servicing Personnel Office Conference held in Topeka, Kansas. Approximately 250 USCG human resource employees were in attendance for the 90 minute presentation.

U.S. Coast Guard (continued)

- USCG held its third annual Privacy Awareness week on November 1-5, 2010. An ALCOAST was sent USCG-wide announcing privacy awareness week and commands were directed to assist in the promotions. During the week at USCG HQ, privacy posters, pamphlets and brochures were on display throughout the building and surrounding area commands. A privacy booth was set up in the HQ cafeteria for three days and a USCG Privacy Analyst was provided to answer questions. The privacy booth was made accessible to several thousand USCG military, contractor and civilian employees. In addition, a one day privacy compliance training session was provided to 50 personnel.

US-VISIT

- US-VISIT held its annual Privacy Awareness week on October 25-29, 2010. Speakers from the DHS Privacy office, Social Security Administration, and the Federal Trade Commission shared their knowledge, expertise, insight and experience on various privacy-related topics such as "International Privacy Issues," "Consumer Protection and Privacy," and "Health Information Technology and Privacy."

IV. 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 table below 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 Act and Privacy Management*. Complaints are received from U.S. citizens and lawful permanent residents as well as visitors and aliens.[5]

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	5	5	0	0
Redress	1	0	1	2
Operational	58	59	6	6
Referred	10	5	5	0
Total	***74***	***69***	***12***	***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.[6]
3. *Operational*. Issues related to general privacy concerns, and concerns not related to transparency or redress.
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 they 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.

[5] *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.*
[6] This category excludes FOIA and Privacy Act requests for access which are reported annually in the Annual FOIA Report.

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

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:

U.S. Customs and Border Protection (CBP)
An individual called the CBP Info Center to file a complaint regarding her treatment during secondary screening. She stated the on-duty officer questioned her about a pending criminal case loudly, in front of other travelers that were waiting to be processed. The individual claimed it was embarrassing, and a violation of her privacy. The Supervisory CBP Officer contacted the individual by telephone and was able to resolve the complaint. The Port Director sent a follow-up letter advising the individual to request to speak to a Passenger Service Manager in the future should she be dissatisfied with the process.

Transportation Security Administration (TSA)
TSA received complaints from individuals who objected to the use of Advanced Imaging Technology (AIT), or objected to any physical screening procedures at airports. Many of the complaints were based on reaction to media coverage rather than personal experience. TSA responded to these complaints by reiterating that the agency adopted privacy safeguards for the use of AIT before the machines were installed, and continues to use comprehensive privacy safeguards in all of its passenger screening methods.

Imaging technology cannot store, export, print, or transmit images. Privacy features blur images to anonymize them. All images are deleted from the system after they are reviewed by the remotely-located operator. In addition, no cameras, cellular telephones, or any device capable of capturing an image is permitted in the resolution room.

After addressing questions regarding AIT technology, TSA placed the individuals in contact with appropriate TSA staffers capable of addressing physical pat-down concerns. In addition, TSA directed the individuals to the TSA AIT website and to ongoing TSA blog discussions addressing specific Thanksgiving Day travel concerns during this reporting period.

U.S. Immigration and Customs Enforcement (ICE)

The ICE Privacy Office received one new privacy complaint concerning the complainant's supervisor and her instruction to refrain from placing personal appointments on the government, Microsoft Outlook calendars. Specifically, the employee objected to being unable to place personal appointments and reminders on the calendar and mark them private so others could not view them. The ICE Privacy Office coordinated with the Office of Professional Responsibility and the Office of Employee & Labor Relations to determine the appropriate response, and then responded directly to the complainant in a letter. The ICE Privacy Office determined the supervisor was within her authority to instruct her employees not to use the Outlook calendar for personal use during the work day because the supervisor used the calendar to determine her staff's availability.