Department of Homeland Security

Privacy Office

First Quarter Fiscal Year 2012 Report to Congress

March 2012

Homeland Security

I. FOREWORD

March 9, 2012

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *First Quarter Fiscal Year 2012 Report to Congress*. This quarterly report includes activities from September 1, 2011 – November 30, 2011.

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[1] (*9/11 Commission Act*) 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; and
- Number and nature of privacy complaints received by DHS for alleged violations along with a summary of the disposition of such complaints.

In addition, we include information and data on privacy training and awareness activities conducted by the Department to help prevent privacy incidents.

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
[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
FIRST QUARTER FISCAL YEAR 2012
SECTION 803 REPORT TO CONGRESS

Table of Contents

II. LEGISLATIVE LANGUAGE

Section 803 of the *9/11 Commission Act*, 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* and the *Homeland Security Act of 2002*, as amended, and by DHS policy;
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 required by Section 804 of the *9/11 Commission Act* [7]; 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 Fiscal Year 2012 Reviews	
Review Type	**# of Reviews**
Privacy Threshold Analyses	109
Privacy Impact Assessments	9
System of Records Notices and Associated Privacy Act Exemptions	11
Privacy Act (e)(3) Statements	3
Computer Matching Agreements	1
Data Mining Reports	0
Privacy Reviews of IT and Program Budget Requests	0
Total Reviews	***133***

[7] 42 U.S.C. §2000ee-3

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 PII. As of November 30, 2011, 81 percent of the Department's Federal Information Security Management Act (FISMA) systems that require a PIA were covered by a PIA, an increase from 80 percent at the end of the fourth quarter of FY 2011. 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.

The following are three examples of PIAs published during this reporting period. All PIAs conducted by DHS can be found on our website, www.dhs.gov/privacy. *Please note that any update to an existing PIA is listed with a small letter after the number for the original PIA.*

DHS/ALL/PIA-013(a) Department of Homeland Security PRISM Update
Background: DHS published this PIA update to reflect changes in the collection of information and the addition of a classified Protective Research Information System Management System (PRISM-ID). PRISM provides comprehensive Federal Acquisition Regulation-based acquisition support for DHS headquarters entities.
Purpose: This PIA was updated because of the new PRISM system that will be implemented for the Department of Homeland Security Office of the Chief Procurement Officer. Additional changes were implemented to restrict access to Taxpayer Identification Numbers to only those users who require it to perform their duties. *(November 10, 2011)*

DHS/ICE/PIA-004(a) ICE Pattern Analysis and Information Collection (ICEPIC) Update
Background: The U.S. Immigration and Customs Enforcement (ICE) published this PIA update to provide transparency related to the Law Enforcement Information Sharing Service (LEIS Service), a web-accessible portal that enables law enforcement agencies outside DHS to query certain information available through ICEPIC. Additionally, DHS law enforcement personnel are able to query external law enforcement agencies' sensitive but unclassified law enforcement information.
Purpose: ICE conducted this PIA update because ICEPIC's sensitive but unclassified DHS law enforcement data can now be accessed by external Federal, state, local, tribal and international law enforcement agency partners (member agencies) through the LEIS Service. *(October 26, 2011)*

DHS/FEMA/PIA/PIA-018 Suspicious Activity Reporting (SAR)
Background: The Federal Emergency Management Agency (FEMA) published this PIA because SAR is designed to collect, investigate, analyze, and report suspicious activities to the Federal Bureau of Investigation, the Joint Terrorism Task Force, the Federal Protective Service, and any other Federal, state, or local law enforcement authorities required to investigate and respond to terrorist threats or hazards to homeland security.
Purpose: FEMA conducted this PIA because the SAR process collects, maintains, and uses PII. FEMA's Office of the Chief Security Officer will collect, maintain, use, and retrieve records on individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged with the investigation, analysis, and appropriate handling of suspicious activity reports. (*September 9, 2011*)

System of Records Notices
In addition to the PIAs published during this reporting period, DHS also published 11 Privacy Act SORNs to support systems at the Department. As of November 30, 2011, 96 percent of the Department's FISMA systems that require a SORN were 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 published during this reporting period. All DHS SORNs can be found on our website, www.dhs.gov/privacy.

- ***DHS/USCG-014 Military Pay and Personnel System of Records Notice***
  United States Coast Guard's (USCG's) System of Records collects and maintains records regarding pay and personnel. As a result of a biennial review of this system, records have been updated in the categories of individuals, records, purpose, and routine uses. This updated system is included in DHS' inventory of record systems. *(October 28, 2011)*

- ***DHS/USSS-003 Non-Criminal Investigation Information System***
  United States Secret Service's (USSS's) System of Records has been updated within the categories of individuals covered in the system and categories of records in this system in order to further define and narrow categories. One routine use was revised to further define the purposes of disclosure, and retention and disposal procedures were updated to reflect current retention practices. The notification procedures were updated to clarify the reason for exemption and the method for obtaining access. DHS previously published a Final Rule in the *Federal Register* to exempt this system of records from certain provisions of the Privacy Act. The current updates to this system of records do not impact the nature of the exemptions claimed; the system is included in DHS' inventory of records. *(October 28, 2011)*

- ***DHS/CBP-003 Credit/Debit Card Data System***
  The system allows U.S. Customs and Border Protection to collect, use, and maintain records related to any credit and debit card transactions which it has with individuals. Additionally, DHS issued a Notice of Proposed Rulemaking to exempt the system of records from certain provisions of the Privacy Act, concurrent with the system of records notices published elsewhere in the *Federal Register*. The newly-established system is included in DHS' inventory of records systems. *(November 2, 2011)*

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

- **64,910** DHS personnel and contractors completed the mandatory computer-assisted privacy training course, *Culture of Privacy Awareness* (note: this is an annual requirement).
- **1,631** 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, 88 people were trained in 3 sessions at 3 fusion centers.
- 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*.
    - During this reporting period, 40 analysts were trained on privacy issues related to suspicious activity reporting.

B. DHS Privacy Office Awareness & Outreach

Publications

DHS Privacy Office 2011 Annual Report to Congress – On September 22, 2011, the DHS Privacy Office delivered its Annual Report to Congress. The Annual Report (covering July 1, 2010 to June 30, 2011) details improvements the Privacy Office has made in strengthening privacy protections across the Department's operations, while simultaneously fulfilling the Administration's goals of transparency, public participation, and collaboration. This publication can be found on our website, www.dhs.gov/privacy.

Outreach

The DHS Privacy Office organized two outreach events open to all federal workers during this reporting period:

- *DHS Privacy Office Speaker Series* – The DHS Privacy Office launched a new series of speaking events for the period July 2011 through April 2012.
    - On October 4, 2011, the Chief Privacy Officer hosted a presentation entitled *Issues on the Edge: Nothing to Hide?* featuring George Washington University law professor Daniel Solove.
- *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 workshops on current privacy topics.
    - On September 21, 2011, the CIO International Privacy Subcommittee sponsored an international privacy training forum coordinated by the DHS Privacy Office's International Privacy Policy Director, entitled *Privacy Worldwide: An Introduction to the Global Privacy Debate.*

Meetings & Events

- Privacy Information for Advocates Meeting – On September 16, 2011, the Chief Privacy Officer hosted this quarterly meeting, which is designed to proactively engage the privacy community on current privacy issues.
- Data Privacy and Integrity Advisory Committee (DPIAC) – On October 5, 2011, the DPIAC held its first FY 2012 quarterly meeting in Arlington, VA. Following the Chief Privacy Officer's update, the committee discussed two draft reports prepared by the subcommittees on privacy protections for information sharing within the Department. The committee also heard a presentation on DHS Freedom of Information Act (FOIA) operations by the Deputy Chief FOIA Officer, and a presentation by the Transportation Security Administration's (TSA) Director of Privacy and Compliance on the Department's use of Automated Target Recognition software to screen travelers at airports.
- National Protection and Programs Directorate (NPPD) Privacy Week – On October 24, 2011, the Chief Privacy Officer gave the keynote address for NPPD's Privacy Week kick-off event. She spoke about the importance of protecting PII, and gave examples of PIAs relevant to the 100 people who attended.

- International Conference of Data Protection and Privacy Commissioners (ICDPPC) – On November 2–3, 2011, the Chief Privacy Officer and the International Privacy Policy Director traveled to Mexico City for the 33rd annual International Conference of Data Protection & Privacy Commissioners. The Chief Privacy Officer participated in two panel discussions: *Privacy by Design in the Public Sector*, and *Data Protection Agency Oversight of Privacy at Law Enforcement Agencies*. The Director participated on a panel discussion about the use of social media in emergency situations.

C. Component Privacy Office Awareness & Outreach

National Protection and Programs Directorate Privacy Office
NPPD Privacy engaged in the following activities this quarter:

- Held its first directorate-wide Privacy Awareness Week in October. The event coincided with National Cybersecurity Awareness Month. The theme was "Our Shared Responsibility," emphasizing that all individuals have a role in protecting personal data and furthering NPPD's commitment to ensuring its employees employ safe information handling practices at work and at home. *Privacy Week* was an overwhelming success, drawing over 300 participants from across the directorate, as well as from other components of the Department.
- Launched the *Privacy Update*, a quarterly publication aimed at increasing overall awareness of privacy within the NPPD community.
- Kicked off a Social Media Working Group, comprised of representatives of offices across the directorate, to identify and assist with privacy-related policies and procedures for the use of social media in the NPPD work environment.
- Developed and disseminated guidance on best practices for safeguarding personally identifiable information while teleworking, which became the model for a DHS-wide teleworking factsheet.
- Created a business-card size privacy incident guide that is now distributed to all on-boarding NPPD employees during orientation. The card fits nicely inside employees' badge-holders and serves as an easy reference to employees on how to respond in the event of a suspected or confirmed privacy incident.

Transportation Security Administration Privacy Office
The TSA Privacy Officer:

- Participated in the DHS Cyber Security Conference, October 3-6, 2011, in Baltimore, Maryland.
- Participated in a conference call with all Federal Security Directors on privacy policy and compliance.
- Made presentations to the Privacy Coalition, the Privacy Information for Advocates Meeting, and at the DPIAC meeting.
- Provided an overview of aviation security to a local middle school debate team.

United States Coast Guard Privacy Office
The USCG Privacy Officer:

- Attended the e-Discovery Readiness for Government Conference on November 29, 2011, in Arlington, Virginia. During the conference, more than 45 senior government experts discussed the E-Discovery Readiness for Government programs.

U.S. Immigration & Customs Enforcement Privacy Office

- ICE Privacy presented at the Human Rights Law Conference, discussing privacy and information sharing on September 14, 2011, in Reston, Virginia. Approximately 250 agents and attorneys from ICE, DHS, and the Department of Justice attended.
- ICE Privacy Officer presented at the Office of Professional Responsibility Leadership Conference discussing privacy at ICE on September 14, 2011, in Arlington, Virginia.
- ICE Privacy recorded a video clip on Sensitive PII that was broadcast for all ICE employees during Cyber Security Month in October.

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, and aliens.[8]

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	4	3	2	0
Redress	4	3	2	0
Operational	285	301	27	13
Referred	2	1	1	0
Total	***295***	***308***	***32***	***13***

*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.[9]
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.

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

[9] This category excludes Freedom of Information Act and Privacy Act requests for access, which are reported annually in the Annual FOIA Report, and 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:

U.S. Customs and Border Protection

Complaint: The CBP INFO Center was contacted by a physician who is a United States citizen. He complained that when he travels abroad to practice medicine, he is questioned about the diseases he may have or has had. He was also dissatisfied that his laptop computer was confiscated briefly and examined during his questioning. He considered this to be a breach of The Health Insurance Portability and Accountability Act (HIPAA) because he stores patient information on his laptop computer.

Disposition: The complainant was informed of the routine questions asked of all international travelers entering or returning to the United States, including "Do you have a communicable disease…?" CBP also provided the complainant a copy of its traveler "tear sheet", which describes its search authority regarding electronic devices,[10] and explained that CBP does not retain copies of any information reviewed unless it is necessary for prosecution.

Complaint: The CBP INFO Center was contacted by a female traveler who was selected for secondary inspection at a land border crossing. She was informed by the CBP officer that he needed to search her vehicle. The officer asked to see her cell phone and asked for an oral declaration regarding the contents of the vehicle. The complainant asked if it was legal to have her phone searched without her being present and was given a traveler "tear sheet" explaining CBP's search authority regarding electronic devices. The complainant was still asking why the officers were checking her phone when she was told to be quiet. She said that her phone was tampered with and she thinks something was copied and perhaps placed on the internet. The complainant also said she was treated rudely and felt her rights had been violated.

Disposition: A letter was sent to the complainant informing her that the officers involved were spoken to about their professionalism, along with another copy of the traveler "tear sheet" explaining CBP's search authority regarding electronic devices, which states that CBP does not retain copies of any information reviewed.

[10] CBP's border search authority of electronic devices emanates from multiple sections of Titles 8 and 19 of the U.S.C., as well as §401 in Title 22 and §5317 in Title 31.

Federal Emergency Management Agency

Complaint: In October 2011, FEMA disseminated correspondence through the mail to various FEMA employees asking them to verify their employee-related personal information. The correspondence included a privacy notice and detailed employment information such as: name, address, pay grade, position title, tax information, etc. On October 27, 2011, a FEMA employee submitted an operational complaint regarding the employee verification correspondence she received in the mail. With identity theft on the rise, the complainant was concerned that her information could have been accessed by an unauthorized person by way of a postal service delivery mistake. The individual asked if it was possible for FEMA to discontinue sending her correspondence through the mail.

Disposition: FEMA-Privacy responded by thoroughly researching the processes and procedures for mailing employee information and determined that FEMA had followed the proper procedures. FEMA Privacy provided recommendations to the individual on how she could reduce the risk of compromise, which alleviated her concerns. The employee was satisfied with the recommendations and the complaint was closed.

U.S. Immigration & Customs Enforcement

Complaint: An ICE employee submitted a two-part privacy complaint. First, the employee alleged that a non-supervisory individual disclosed information regarding the complainant's time and attendance records to employees who did not have a need to know. The employee also alleged that reports on other employees' time and attendance, including their names, hours worked, compensatory time, and overtime, were generated and disclosed by a co-worker at the request of his supervisor.

Disposition: ICE Privacy responded directly to the complainant, inquiring about additional details to better understand the complaint and the timing of the two allegations. The complainant replied that the first incident was resolved in 2009 when she spoke with the non-supervisory individual and requested that she not discuss time and attendance records in a public area. The second incident involving the release of time and attendance data was resolved by the office director in 2011. The director advised that the reports were in violation of privacy requirements and requested that they be discontinued. ICE Privacy determined that no further action was necessary since both incidents were managed internally by the program office. ICE Privacy sent the complainant an email stating that the complaint had been closed, along with the reasons.

Transportation Security Administration

Complaint: TSA received a complaint from a traveler who believed TSA violated her privacy by asking questions as part of a pilot program using Behavior Detection Officers (BDO). BDOs engage travelers in a brief conversation during which they use behavioral observations to identify potentially higher-risk individuals. She also stated that she believed that TSA subjected her to a pat-down in retaliation for expressing disagreement with the pilot program.

Disposition: TSA thanked the passenger for her input, and concluded that the incident revealed that communications between a traveler and BDO might be improved when it is apparent that a traveler is uncomfortable answering questions for reasons that appear to be unrelated to a security threat and will use this incident to improve its BDO training. TSA informed the complainant that the pat-down was prompted by the magnetometer alarm, and that the alarm could not be prompted by security officers.