Department of Homeland Security

Privacy Office

First Quarter Fiscal Year 2013 Report to Congress

March 2013

Homeland Security

I. FOREWORD

March 31, 2013

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *First Quarter Fiscal Year 2013 Report to Congress*. This quarterly report covers the activities listed below from September 1, 2012 – November 30, 2012.[1]

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[2] (9/11 Commission Act) requires the DHS Privacy Office to report quarterly on the following activities:

- 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. Section 222 of the *Homeland Security Act of 2002* (Homeland Security Act),[3] sets forth the responsibilities of the DHS Privacy Office. The mission of the DHS Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. Within DHS, the Chief Privacy Officer implements Section 222 of the Homeland Security Act, the *Privacy Act of 1974*[4] (Privacy Act), the *Freedom of Information Act*[5] (FOIA), and the *E-Government Act of 2002*[6] (E-Government Act), along with numerous other laws, executive orders, court decisions, and DHS policies that impact the collection, use, and disclosure of personally identifiable information (PII) by DHS.

[1] The reporting period for this report corresponds with the period established for reporting under *The Federal Information Security Management Act of 2002* (FISMA, 44 U.S.C. § 3541) rather than the October through September fiscal year.
[2] 42 U.S.C. § 2000ee-1(f).
[3] 6 U.S.C. § 142.
[4] 5 U.S.C. § 552a.
[5] 5 U.S.C. § 552.
[6] 44 U.S.C. § 101 note.

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

The Honorable Thomas R. Carper
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Coburn, M.D.
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 Michael McCaul
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 Bob Goodlatte
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

Please direct any inquiries about this report to the DHS Privacy Office at 202-343-1717 or privacy@dhs.gov. This report and other information about the Office are available on our website, listed below.

Sincerely,

Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security

DHS PRIVACY OFFICE
FIRST QUARTER FISCAL YEAR 2013
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, sets forth the following requirements:

"(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 programs and information technology (IT) systems that may have a privacy impact.

For purposes of this report, reviews include the following DHS Privacy Office 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), as required under the E-Government Act, the Homeland Security Act,[7] and DHS policy;

3. System of Records Notices (SORN), as required under the Privacy Act[8] and associated Privacy Act exemptions;[9]

4. Privacy Act Statements, as required under the Privacy Act[10] to provide notice to individuals at the point of collection;

5. Computer Matching Agreements, as required under the Privacy Act;[11]

6. Data Mining Reports, as required by Section 804 of the 9/11 Commission Act; [12]

7. Privacy Compliance Reviews, per the authority granted to the DHS Chief Privacy Officer by the Homeland Security Act;

8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board; and

9. Other privacy reviews, such as implementation reviews for information sharing agreements.

[7] 6 U.S.C. § 142.
[8] 5 U.S.C. § 552a(e)(4).
[9] 5 U.S.C. § 552a(j), (k).
[10] 5 U.S.C. § 552a(e)(3).
[11] 5 U.S.C. § 552a(o)-(u).
[12] 42 U.S.C. § 2000ee-3.

Table I: Reviews Conducted During First Quarter Fiscal Year 2013	
Review Type	**Number of Reviews**
Privacy Threshold Analyses	163
Privacy Impact Assessments	13
System of Records Notices and Associated Privacy Act Exemptions	3
Privacy Act (e)(3) Statements	16
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Compliance Reviews	2
Privacy Reviews of IT and Program Budget Requests	1
Other Privacy Reviews	1
Total Reviews	***199***

A. Privacy Impact Assessments

The Privacy Impact Assessment (PIA) process is one of the Department's key mechanisms to ensure that DHS programs and technologies sustain, and do not erode, privacy protections for the use, collection, and disclosure of PII. As of November 30, 2012, 85 percent of the Department's Federal Information Security Management Act (FISMA) systems requiring a PIA had one in effect.

In addition to completing PIAs for systems not currently subject to a PIA, the Department conducts a triennial review of existing PIAs to assess and confirm that the systems still operate within the originally published parameters. After the Department completes a triennial review, it updates any previously published PIAs to inform the public that it has completed a review of the affected systems.

The Department published 13 new or updated PIAs during the reporting period, and each is summarized below. Updates to existing PIAs appear with a lower-case letter in parentheses after the original PIA number. All PIAs are available on our website, www.dhs.gov/privacy.

DHS/S&T/PIA-024 Rapid DNA System Test and Evaluation
Background: DHS's Science and Technology Directorate (S&T) developed the Rapid Deoxyribonucleic Acid (DNA) System to meet a need stated by U. S. Citizenship and Immigration Services (USCIS) to verify family relationships (kinship) in refugee immigration processes. The Rapid DNA System performs rapid, low-cost DNA analysis to meet this USCIS need and may also address the operational needs of other DHS components.

Purpose: S&T conducted this PIA because the collection and analysis of DNA information may have an impact on privacy and raises privacy concerns. The Rapid DNA System has access control, encryption, and other privacy-protective measures built in. For example, each Rapid DNA System operator has a unique account to access the system, and is required to sign into the system with a DHS-issued credential and corresponding PIN. System audit and usage logs document individual logins and uses for security purposes, as well as for identification of training and performance issues with the prototype system. The resulting DNA profile data is encrypted within the system. The prototype conducts all of the processing internally and does not have the ability to transmit data electronically. *(September 14, 2012)*

DHS/TSA/PIA-038 Performance and Results Information System
Background: Transportation Security Administration's (TSA) Performance and Results Information System (PARIS) database maintains information associated with TSA's regulatory investigations, security incidents, and enforcement actions, and records the details of security incidents involving passenger and property screening.

Purpose: PARIS maintains PII on individuals, including witnesses involved in security incidents or regulatory enforcement activities. PARIS also creates and maintains a list of individuals who, based upon their involvement in security incidents of sufficient severity or frequency, are disqualified from receiving expedited screening. This PIA informs the public of changes in the use of PARIS and any resulting impact on personal privacy. *(September 18, 2012)*

DHS/CBP/PIA-004(f) - Western Hemisphere Travel Initiative: Beyond the Border Entry/Exit Program Phase I

Background: This update describes Phase I of the Beyond the Border entry/exit program, an initiative of the U.S.-Canada Beyond the Border Action Plan. The Beyond the Border entry/exit program will expand the sharing of border crossing information with the Canada Border Services Agency (CBSA) by exchanging biographic, travel document, and other border crossing information collected from individuals entering the United States from Canada and, vice versa, at land ports of entry.

Purpose: This PIA update covers Phase I of the entry/exit program only, which is limited to exchanging entry records from certain individuals (other than U.S. and Canadian citizens) at certain land ports of entry to measure the ability to reconcile biographic entry records between Canada and the United States. DHS will publish additional updates to this PIA prior to deploying any future phases to the Beyond the Border entry/exit program. *(September 24, 2012)*

DHS/S&T/PIA-025 Gaming System Monitoring and Analysis Effort

Background: The Gaming System Monitoring and Analysis project is a research effort funded by the S&T Directorate's Cyber Security Division (CSD) to design and develop forensic tools for extracting data from standalone gaming systems. .

Purpose: S&T conducted this PIA because gaming systems used in this research project may contain PII. The Naval Postgraduate School (NPS) is conducting the research. NPS restricts its purchasing of used gaming consoles to systems that have been sold or disposed of by their previous owners outside the United States. Previous experience has shown that used equipment purchased inside the U.S. is highly likely to contain U.S. Person data, while equipment purchased outside the U.S. is less likely to contain such data. As a second level of protection, NPS researchers and NPS contractors protect the information using access control technologies and generally do not attempt to identify any individuals whose information may reside inside the data carrying devices. For most of the project, data is used in aggregate form where it is processed and analyzed in bulk. *(October 11, 2012)*

DHS/FEMA/PIA-011 National Flood Insurance Program Information Technology System

Background: The Federal Emergency Management Agency (FEMA) Federal Insurance and Mitigation Administration (FIMA) National Flood Insurance Program (NFIP) owns and operates the NFIP Information Technology System (ITS). This system processes certain flood insurance policies and claims, including those from the FEMA Direct Servicing Agent (DSA) contractor on behalf of the NFIP, and by Write Your Own Companies (WYO), which sells and services flood insurance policies.

Purpose: FEMA conducted this PIA because the system collects, uses, maintains, retrieves, and disseminates PII from individuals who either purchase or process flood insurance policies from NFIP, as well as from individuals who request access to the system. *(October 12, 2012)*

DHS/ICE/PIA-032(a) FALCON Search & Analysis System

Background: U.S. Immigration and Customs Enforcement (ICE) agents, criminal research specialists, and intelligence analysts use the FALCON Search & Analysis System (FALCON-SA) to conduct research that supports the production of law enforcement intelligence products, provides lead information for investigative inquiry and follow-up, assists in the conduct of ICE criminal and administrative investigations and in the disruption of terrorist or other criminal activity, and discovers previously unknown connections among existing ICE investigations.

Purpose: This PIA re-publication makes minor changes to the original FALCON-SA PIA (February 1, 2012), including updated appendices to address the addition of tip records from FALCON Tipline as records routinely ingested into FALCON-SA. *(November 2, 2012)*

DHS/ICE/PIA-033 FALCON Tipline (FALCON-TL)
Background: ICE Homeland Security Investigations (HSI) has deployed a new information system called FALCON Tipline (FALCON-TL), a component system of the larger HSI FALCON environment. This workflow management system supports the creation and maintenance of tips received by the HSI Tipline Unit about suspicious activity or suspected illegal activity, and the referral of this information to HSI field offices for investigation or other follow up.

Purpose: This PIA is necessary because FALCON-TL maintains PII about both the individuals who report the tips and the individuals who are the subject of the tips. *(November 2, 2012)*

DHS/TSA/PIA-039 Office of Intelligence & Analysis Trends and Patterns Branch (TPB)
Background: TSA's Trends and Patterns Branch (TPB) seeks to improve the ability to identify potential risks to transportation security by discovering and analyzing previously unknown links or patterns among: (1) individuals who undergo a TSA security threat assessment; (2) aviation passengers identified as a match to a watch list; and (3) passengers who do not present acceptable identification documents in order to access the sterile area of an airport.

Purpose: TSA conducted this PIA because TPB collects and uses PII to perform these functions. *(November 14, 2012)*

DHS/TSA/PIA-040, Port Authority of New York/New Jersey Secure Worker Access Consortium Vetting Services (SWAC)
Background: TSA conducts Federal Government watch list checks of workers at Port Authority of New York/New Jersey (PANYNJ) facilities and job sites, including airports, marine ports, bus terminals, rail transit facilities, bridges, tunnels, and real estate such as the World Trade Center memorial site. TSA also conducts terrorism watch list checks of individuals identified by PANYNJ as requiring such checks for access to sensitive information, and for workers at facilities and job sites of PANYNJ's regional partners.

Purpose: TSA conducted this PIA because PII is collected during Federal Government watch list checks of workers at PANYNJ facilities and job sites. *(November 14, 2012)*

DHS/FEMA/PIA-012(a) Disaster Assistance Improvement Program (DAIP)
Background: FEMA's Office of Response & Recovery (OR&R), Recovery Directorate, National Processing Service Center (NPSC) Operations Branch, sponsors and funds the DAIP. The DAIP developed the Disaster Assistance Center (DAC) system to maintain disaster survivor application and registration information collected through various media.

Purpose: FEMA conducted this PIA because the DAC collects, uses, maintains, retrieves, and disseminates the PII of disaster survivors who request government benefits. *(November 16, 2012)*

DHS/S&T/PIA-026 Robotic Aircraft for Public Safety (RAPS) Project
Background: The S&T Directorate and the State of Oklahoma are partnering on the Robotic Aircraft for Public Safety (RAPS) project to test and evaluate Small Unmanned Aircraft Systems (SUAS) for potential use by the first responder community and DHS operational components. SUAS includes small aircraft that are operated using a wireless ground control station (GCS). These aircraft are equipped with sensors and cameras that can capture images and transmit them to a ground control system to provide aerial views of emergency situations and for situational awareness.

Purpose: S&T conducted this PIA to address the privacy impacts of the system's surveillance and image capturing capabilities. During the tests, the images captured by the SUAS are transmitted and stored on the GCS, which includes a standalone laptop. The GCS has access controls in place that ensure that only those with an authorized need to know (S&T RAPS team) can access the images. The RAPS team stores images under password protection and immediately deletes any images that unintentionally captured private citizens or property during the course of the testing. As the technology continues to mature and develop, the privacy risks and concerns will evolve as well. To proactively address these concerns and risks, DHS is establishing a UAS issue working group to explore departmental roles and equities involving privacy and civil liberties. The working group aims to identify and address privacy and civil liberties issues related to DHS uses of UAS by providing policies, procedures, and best practices. The working group will produce a white paper that contains further privacy analysis and recommendations that can be used as best practices or foundational principles for other federal, state, and local government users, as well as non-government users. *(November 16, 2012)*

DHS/USCG/PIA-001(b) Homeport Internet Portal Update
Background: The United States Coast Guard (USCG) currently uses the Homeport Internet Portal to provide: (1) secure information dissemination; (2) advanced collaboration for Area Maritime Security Committees (AMSC); (3) electronic submission and approval for facility security plans; and (4) complex electronic notification capabilities.

Purpose: USCG issued this PIA update to include TSA operations center personnel as authorized users of Homeport's Alert Warning System, which contains non-Sensitive PII and disseminates airport security information to authorized recipients. *(November 16, 2012)*

DHS/ICE/PIA-029 ICE Alien Medical Records Systems
Background: Aliens held in custody at a facility staffed by the ICE Health Services Corps (IHSC) receive physical exams and treatment, dental services, and pharmacy services, depending on an alien's medical condition and length of stay. This PIA was originally published on July 25, 2011, and described the information in these medical record systems, the purposes for which this information was collected and used, and the safeguards ICE implemented to mitigate the privacy and security risks to the PII stored in these systems.

Purpose: ICE republished this PIA in full primarily to modify the description of the MedPAR system, which originally was to be hosted by the U.S. Department of Veterans Affairs but will now remain at ICE. *(November 27, 2012)*

B. System of Records Notices

As of November 30, 2012, 96 percent of the Department's FISMA systems that require a System of Records Notice (SORN) had an applicable SORN. SORNs 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 original SORN remains in effect.

DHS SORNs and Final Rules for Privacy Act exemptions are available on our website, www.dhs.gov/privacy.

During the reporting period, DHS published three SORNs, summarized below.

DHS/ICE-005 - Trade Transparency Analysis and Research (TTAR)
The data in the TTAR system of records is generally maintained in the ICE Data Analysis and Research Trade Transparency System (DARTTS), a software application and data repository that analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. This system of records was modified to include new categories of individuals, records, and purposes. The system has also been updated to consolidate and clarify the existing routine uses, to reflect a proposed change to the retention period of the system's data, and to simplify the description of the record sources.
(77 Fed. Reg. 53893 (Sep. 4, 2012))

DHS/ALL - 004 General Information Technology Access Account Records System
This system comprises information collected to provide authorized individuals with access to DHS information technology resources, including user name, business affiliation, account information, and passwords. Passwords are encrypted and used as part of the log in process for verification of appropriate access. After a biennial review of this system, the Department updated the categories of individuals to include individuals who have been denied system access or had their access revoked. In addition, the categories of records has been updated to include such information as voluntary posting of photos for collaboration purposes, comments posted for collaboration purposes, training taken, justification for access, and all logs of activity on the DHS network.
(77 Fed. Reg. 70792 (Nov. 27, 2012))

DHS/TSA 019 - Secure Flight Records
TSA is republishing this SORN to reflect additions to TSA's screening capabilities designed to better focus enhanced passenger screening efforts on individuals likely to pose a threat to civil aviation, and to facilitate the secure and efficient travel of the vast majority of the traveling public by distinguishing them from individuals on Federal Government watch lists. This SORN includes modifications in the following areas of the SORN: categories of individuals, categories of records, purpose(s), routine uses, disclosure to consumer reporting agencies, data retention and disposal, notification procedure, records access procedures, and the record source categories.
(77 Fed. Reg. 69491 (Nov. 19, 2012))

C. Privacy Compliance Reviews

The DHS Privacy Office uses Privacy Compliance Reviews (PCR) to ensure DHS programs and technologies implement and maintain appropriate privacy protections for PII. Consistent with the DHS Privacy Office's unique position as both an advisor and oversight body for the Department's privacy-sensitive programs and systems, the PCR is a collaborative effort that helps improve a program's ability to comply with existing privacy compliance documentation, including PIAs, SORNs, and formal agreements such as Memoranda of Understanding or Memoranda of Agreement.

Reports on the results of PCRs are available on our website, www.dhs.gov/privacy, under "Investigations and Compliance Reviews."

During this reporting period, the DHS Privacy Office completed two PCRs:

1. DHS completed a multi-component review of DHS's participation in the Nationwide Suspicious Activity Reporting Initiative (NSI), resulting in a letter to the program principal. The letter identifies lessons learned and recommendations for strengthening DHS's participation in the NSI.

2. DHS completed a fifth PCR on the on the Office of Operations Coordination and Planning National Operations Center's (OPS/NOC) Publicly Available Media Monitoring and Situational Awareness Initiative, and issued a publicly available report on the results of the review on November 7, 2012. The PCR found continued compliance with the January 2011 PIA Update and the February 2011 SORN.

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

Mandatory Training

75,852 DHS personnel completed the mandatory computer-assisted privacy awareness training course, *Privacy at DHS: Protecting Personal Information*. This course is required for all personnel when they join the Department, and annually thereafter.

New Employee Training

2,261 DHS personnel attended instructor-led privacy training courses, primarily privacy training for new employees:

- The DHS Privacy Office provides introductory privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees.
- The DHS Privacy Office provides privacy training each month as part of the two-day *DHS 101* course, which is required for all new and existing headquarters staff.
- Many of the Component Privacy Officers[13] also offer introductory privacy training for new employees.

Fusion Center Training

- The DHS Privacy Office collaborates 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 the reporting period, DHS trained:
        - 83 people in 3 sessions at 3 fusion centers;
        - 113 people at the National Fusion Center Privacy and Civil Rights and Civil Liberties Workshop held in Nashville, Tennessee on November 14-15.

Compliance Training

- Beginning October 24, 2012, the DHS Privacy Office Compliance Team led an intensive eight-week compliance boot camp training program for new compliance analysts and privacy analysts from USCIS, TSA, and US-VISIT. At each session, 8-10 trainees practiced using the Fair Information Practice Principles to analyze privacy risk and determine privacy compliance documentation requirements.

[13] 10 DHS offices and components have a Privacy Officer.

B. DHS Privacy Office Awareness & Outreach

Meetings & Events

- *Government Series (GS) 0306 What Does It Really Mean?* Training Seminar – On October 18, the Deputy Chief FOIA Officer spoke at the American Society of Access Professionals (ASAP) luncheon seminar, discussing how the DHS Privacy Office has benefited from the new Government Information Specialist (GS) 0306 series.
- National Protection and Programs Directorate's (NPPD) Privacy Awareness Week – On October 22, the Acting Chief Privacy Officer gave the keynote presentation.
- Data Privacy & Integrity Advisory Committee (DPIAC) Meeting – On November 7, the DPIAC held a public meeting in Washington, DC to consider best practice recommendations for DHS cybersecurity pilots and biometrics collection and use. Following the Acting Chief Privacy Officer's update, the Committee received a comprehensive cybersecurity overview from the Director of Network Security Deployment.
- Committee on Homeland Security (CHS), Subcommittee on Transportation Security Hearing: Transportation Security Administration (TSA) Recent Scanner Shuffle: Real Strategy or Wasteful Smokescreen? – On November 15, the Acting Chief Privacy Officer and TSA's Assistant Administrator, Office of Security Capabilities, testified before the CHS, Subcommittee on Transportation Security, to address privacy and health concerns related to Advanced Imaging Technology.
- Privacy Coalition Meeting – On November 30, the Acting Chief Privacy Officer was the keynote speaker at the Electronic Privacy Information Center's (EPIC) Privacy Coalition Meeting. He led a discussion among members of the privacy and transparency advocacy community on the Senate Permanent Subcommittee on Investigations' recent report on Fusion Centers, as well as on Freedom of Information Act management issues.

C. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency (FEMA) Privacy Office

- Provided specialized privacy awareness training to personnel in the Human Capital Division and the Office of Equal Rights at FEMA Headquarters, and also to personnel at the Virginia National Processing Service Center (NPSC) in Winchester, Virginia.
- Conducted privacy site inspections at the Maryland NPSC in Hyattsville, Maryland; Virginia NPSC in Winchester, Virginia; and the Human Capital Division at FEMA Headquarters.

National Protection and Programs Directorate (NPPD) Office of Privacy

- Participated in the Federal CIO Council's Coffee Talk events, sharing best practices for training human resource professionals on privacy, and planning a privacy awareness event.
- Co-hosted privacy and civil rights and civil liberties training with the DHS Office for Civil Rights and Civil Liberties on October 4, emphasizing what employees and contractors should be aware of when developing and reviewing external products. NPPD Privacy created a new external product checklist to help employees evaluate privacy and civil rights and civil liberties concerns.
- Hosted an event titled "*Got Cookies?*" to increase awareness of its upcoming Privacy Week event, as well as educate employees about the privacy risks associated with web cookies. During this event, NPPD Privacy distributed a fact sheet on cookies, as well as other privacy awareness materials.
- Hosted its second annual Privacy Awareness Week, "Privacy by Design: We Bake Privacy Protections into Everything We Do," from October 22-26. Over 275 employees attended, learning ways to effectively 'bake' or incorporate privacy protections into everything from program inception to system design to employees' day-to-day activities.
- Provided a privacy briefing on November 1, during the quarterly Contracting Officer Representatives' Meeting, to introduce guidance on privacy provisions for NPPD solicitations and statements of work, as well as privacy tips for contracting officer representatives.
- Provided specialized privacy training to the Office of Cybersecurity and Communications' Information Assurance team on November 30.
- Released new guidance titled "How to Incorporate the Fair Information Practice Principles into Correspondence and Task Management," targeting the information management and executive secretariat community.
- Distributed specialized guidance to Combined Federal Campaign (CFC) leads and key workers on safeguarding PII in connection with the collection of CFC pledge materials, to include instructions on handling privacy incidents, should they occur.
- NPPD published a new issue of the Privacy Update, a quarterly publication aimed at increasing overall awareness of privacy within the NPPD community, with a focus on privacy awareness activities.
- Distributed three privacy tips and one privacy trivia question to all employees in US-VISIT. The privacy tips have increased awareness about safe Smartphone habits, using strong passwords, and reminding employees to lock their computer screens.

Transportation Security Administration (TSA) Privacy Office

- Met with representatives of the Electronic Privacy Information Center to discuss Advanced Imaging Technology.
- Presented DHS and TSA privacy policies to contractors at DeLoitte and General Dynamics during a meeting regarding a technology deployment.
- Presented DHS and TSA privacy policies to human resource officials during a TSA field counsel conference call.
- Distributed an email message to all employees on how to protect email attachments containing Sensitive PII.

U.S. Coast Guard (USCG) Privacy Office

- Staffed privacy information booths in several locations on October 24 and 25 to heighten privacy awareness among employees in preparation for a move to a new central office location in Washington, DC.

U.S. Immigration and Customs Enforcement (ICE) Privacy Office

- Presented on Privacy Act disclosures and ICE privacy policies at the ICE Office of the Public Advocate Team Retreat on October 25.

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*. U.S. citizens, Legal Permanent Residents, visitors, and aliens submit complaints.[14]

Table II: Type and Disposition of Complaints Received in the Reporting Period

Type of Complaint	Number of complaints received during the reporting period	Disposition of Complaint		
		Closed-Responsive Action Taken	In-Progress (Current Period)	In-Progress (Prior Periods)
Process & Procedure	5	6	0	1
Redress	1	1	0	0
Operational	604	569	58	66
Referred	0	0	0	0
Total	***610***	***576***	***58***	***67***

.

DHS separate complaints into four categories:

1. ***Process and Procedure****:* Issues concerning process and procedure, such as consent, or appropriate notice at the time of collection.
    a. *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 and/or correction of PII, and appropriate redress of such issues.
    a. *Example*: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[15]
3. ***Operational***: Issues related to general privacy concerns, and concerns not related to transparency or redress.
    a. *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 internal referrals within DHS. The referral category both serves as a category of complaints and represents

[14] See *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*.
[15] This category excludes FOIA 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.

responsive action taken by the Department, unless a complaint must first be resolved with the external entity.

   a. *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.

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 took responsive action. 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 (TSA)

Complaint: TSA received a complaint from an airline passenger stating that TSA employees collected his PII during an airport checkpoint encounter without providing a proper Privacy Act statement explaining the purpose and authority for collecting the data.

Disposition: The TSA Privacy Office contacted TSA management at the airport in question and determined that the individual raised security concerns after becoming confrontational with TSA personnel during secondary screening. After the confrontation, TSA personnel obtained the individual's name and address in anticipation of initiating an incident report. Privacy Act System of Records DHS/TSA – 001, Transportation Security Enforcement Records System (TSERS) exempts TSA from providing notice to travelers involved in checkpoint incidents. Additional investigation determined that TSA did not prohibit the individual from traveling and never initiated a formal incident report. The TSA Privacy Office advised the passenger of the findings and received a thank you note from him for investigating the encounter.

U.S. Customs and Border Protection (CBP)

Complaint: The CBP INFO Center received a complaint from an individual who regularly passes through a CBP border patrol checkpoint. The complainant reported that his vehicle was routinely stopped at the checkpoint and inspected upon his return, presumably to determine if he was transporting illegal aliens or illegal narcotics. The complainant reported that while he has no objection to such inspections, he does object to the U.S. Border Patrol Agent asking about his travel plans. The complainant maintained that it is inappropriate for U.S. Border Patrol Agents to inquire about travel plans.

Disposition: The CBP INFO Center reviewed this complaint and sent a letter to the individual explaining that Border Patrol Agents are permitted to inquire where travelers intend to go as part of routine questioning, which is within the scope of CBP's authority. The letter further advised that such questions are germane to CBP's ability to identify likely smugglers from the routes most frequently utilized to transport illegal aliens and/or narcotics into the interior of the United States.

Complaint: The CBP INFO Center received a complaint from an individual regarding treatment during processing at a Port of Entry. The complainant, a member of the U.S. military, was asked to present his military ID card and provide his Military Occupation Specialty (MOS). The complainant argued with the CBP Officer and refused to present his military ID. He was then referred for a secondary examination, where his luggage and personal effects were searched. The complainant did not have an issue with being referred for a secondary examination but did object to having to provide the CBP Officer with his military credentials, and requested "clarification and if possible the customs regulation stating that military personnel need to present military ID cards when travelling abroad on personal business, as this is the first time I've been asked to present a military ID when not travelling on official military orders."

Disposition: The CBP INFO Center sent the complainant a letter to explain that while it is within CBP's authority to ask travelers for identification (and therefore the complainant's military ID), CBP does not have a specific regulation to mandate military personnel carry their military ID when not traveling on official orders. The letter also recommended that the complainant request to speak to a supervisor if he encounters problems in the future.

VI. CONCLUSION

As required by the 9/11 Commission Act, this quarterly report summarizes the DHS Privacy Office's activities from September 1, 2012 – November 30, 2012. The DHS Privacy Office will continue to work with Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.