
# Department of Homeland Security

## Privacy Office

## First Quarter Fiscal Year 2014 Report to Congress

*April 2014*

Homeland Security

# Foreword

*April 30, 2014*

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *First Quarter Fiscal Year 2014 Report to Congress* for the period September 1 – November 30, 2013.[1]

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[2] 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 on privacy training and awareness activities conducted by the Department to help prevent privacy incidents.

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] the *Freedom of Information Act*,[5] and the *E-Government Act of 2002*,[6] along with numerous other laws, executive orders, court decisions, and DHS policies that impact the collection, use, and disclosure of personally identifiable information 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, the DHS Privacy Office provides this report 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. More information about the DHS Privacy Office, along with copies of prior reports, is available on the Web at: www.dhs.gov/privacy.

Sincerely,

Karen Neuman
Chief Privacy Officer
U.S. Department of Homeland Security

# DHS PRIVACY OFFICE
# FIRST QUARTER FISCAL YEAR 2014
# SECTION 803 REPORT TO CONGRESS

## Table of Contents


I. FOREWORD ..... 1
II. LEGISLATIVE LANGUAGE ..... 5
III. PRIVACY REVIEWS ..... 6
A. Privacy Impact Assessments ..... 8
B. System of Records Notices ..... 11
C. Privacy Compliance Reviews ..... 12
IV. ADVICE AND RESPONSES ..... 13
A. Privacy Training and Awareness ..... 13
B. DHS Privacy Office Awareness & Outreach ..... 14
C. Component Privacy Office Awareness & Outreach ..... 15
V. PRIVACY COMPLAINTS AND DISPOSITIONS ..... 17
VI. CONCLUSION ..... 20

# II. LEGISLATIVE LANGUAGE

Section 803 of the *9/11 Commission Act of 2007*,[7] 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."

[7] 42 U.S.C. § 2000ee-1.

# III. PRIVACY REVIEWS

The Department of Homeland Security (DHS or Department) Privacy Office (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, 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, as required under the *E-Government Act of 2002*, the *Homeland Security Act of 2002*,[8] and DHS policy;

3. System of Records Notices, as required under the *Privacy Act of 1974*[9] (Privacy Act), and any associated Final Rules for Privacy Act exemptions;[10]

4. Privacy Act Statements, as required under the Privacy Act[11] to provide notice to individuals at the point of collection;

5. Computer Matching Agreements, as required under the Privacy Act;[12]

6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*; [13]

7. Privacy Compliance Reviews, per the authority granted to the DHS Chief Privacy Officer by the *Homeland Security Act of 2002*;[14]

8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 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.

[8] 6 U.S.C. § 142.
[9] 5 U.S.C. § 552a(e)(4).
[10] 5 U.S.C. § 552a(j), (k).
[11] 5 U.S.C. § 552a(e)(3).
[12] 5 U.S.C. § 552a(o)-(u).
[13] 42 U.S.C. § 2000ee-3.
[14] 6 U.S.C. § 142.

| Table I: Reviews Completed First Quarter Fiscal Year 2014 | |
|---|---|
| **Type of Review** | **Number of Reviews** |
| Privacy Threshold Analyses | 127 |
| Privacy Impact Assessments | 18 |
| System of Records Notices and Associated Privacy Act Exemptions | 5 |
| Privacy Act (e)(3) Statements | 0 |
| Computer Matching Agreements | 0 |
| Data Mining Reports | 0 |
| Privacy Compliance Reviews | 0 |
| Privacy Reviews of IT and Program Budget Requests[15] | N/A |
| Other Privacy Reviews | 0 |
| ***Total Reviews*** | ***150*** |

[15] The Chief Information Office prepares a privacy score once a year as part of its Office of Management and Budget Exhibit 300 reporting. Therefore, reviews for this category are calculated only once a year and are included in the fourth quarter report.

# 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. As of November 30, 2013, 91 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 new systems and 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.

During the reporting period, the Office published 18 new, updated, or renewed PIAs. Six PIAs are summarized below, and a hyperlink to the full text of each PIA is included. All published DHS PIAs are available on the DHS Privacy Office website, www.dhs.gov/privacy.

Updates to existing PIAs appear with a lower-case letter in parentheses after the original PIA number.

**DHS/ALL/PIA-046-3** ***Cerberus Pilot (November 22, 2013)***
**Background:** The DHS Cerberus Pilot (Cerberus Pilot) is a part of the overall DHS Data Framework. The goal of the framework is to help alleviate mission limitations associated with stove-piped Information Technology (IT) systems that are currently deployed across multiple operational components at DHS. The Cerberus Pilot is intended to test the feasibility of a more controlled, effective, efficient use and sharing of available homeland security information across the DHS Enterprise, while protecting privacy and safeguarding personal data. During the Cerberus Pilot, the system ingests certain DHS Component unclassified data about individuals, and maintains the data in a DHS-owned and controlled cloud computing environment on a Top Secret/Sensitive Compartmented Information (TS/SCI) network, where it is available for classified searches and evaluation using various analytical tools.

**Purpose:** The goal of the Cerberus Pilot is to test the ability to ensure that only users with certain attributes are able to access data based on defined purposes using the dynamic access control process. The Cerberus Pilot will be populated with data imported from the Neptune Pilot data store via bulk load. The DHS Data Framework and the Neptune Pilot are described in separate PIAs. This PIA was published pursuant to Section 208 of the *E-Government Act of 2002* because the Cerberus Pilot system handles Personally Identifiable Information (PII), and it provides a view into how the Department works to prevent terrorist attacks within the United States, while protecting individual privacy, civil rights, and civil liberties.

**DHS/CBP/PIA-018** ***Aircraft Systems (September 9, 2013)***
**Background:** United States Customs and Border Protection (CBP) is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico, and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard (USCG). To achieve these missions, CBP employs several types of aircraft, including manned helicopters, fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law

enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or other emergencies.

**Purpose:** This PIA addresses the privacy impact of these technologies and provides a level of transparency to the public about the current surveillance programs undertaken by CBP.

**DHS/FEMA/PIA-034** ***Electronic Fingerprint System (EFS) (September 24, 2013)***
**Background:** As required by law, the Federal Emergency Management Agency (FEMA) conducts background investigations of all applicants to ensure that these individuals meet established suitability and security standards. This includes conducting the suitability, clearance, and badging process for FEMA permanent full-time employees, temporary full-time employees, cadres of on-call response employees, reserve employees, contractors, individuals from voluntary organizations, and federal, state, local, and tribal partners working to support FEMA's mission. As part of this process, all applicants undergo a required fingerprint-based criminal history record check. To execute this check, FEMA currently obtains electronic fingerprints and other PII as required by the Federal Bureau of Investigation (FBI) to complete the investigation through its Integrated Automated Fingerprint Identification System (IAFIS).

**Purpose:** This PIA was conducted because the EFS collects PII and leverages the Office of Biometrics and Identity Management's (OBIM) Automated Biometric Identification System (IDENT) to conduct background investigations. This PIA also provides transparency of the process to applicants.

**DHS/TSA/PIA-041** ***TSA Pre✓™ Application Program (September 4, 2013)***
**Background:** TSA Pre✓™ is a passenger pre-screening initiative that allows low-risk passengers who are eligible to receive expedited screening at participating U.S. airport security checkpoints for domestic and international travel. The Transportation Security Administration (TSA) will conduct security threat assessments on individuals who apply to TSA for enrollment into the TSA Pre✓™ Application Program. In an effort to expand the availability of TSA Pre✓™ to other populations, TSA will now conduct security threat assessments on individuals who voluntarily apply to TSA for participation in the TSA Pre✓™ Application Program. The assessment will include checks against law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history records check (CHRC) conducted through the Federal Bureau of Investigation (FBI). The results will be used by TSA to decide if an individual poses a sufficiently low risk to transportation or national security to be issued a Known Traveler Number (KTN). Fingerprints are expected to be enrolled with the FBI for recurrent CHRCs. The FBI will also check fingerprints against its unsolved crimes database, but the result will not be returned to TSA. TSA expects that, in the future, fingerprints will also be enrolled with the National Protection and Programs Directorate/Office of Biometrics Identity Management (NPPD/OBIM) Automatic Biometric Identification System (IDENT) biometric database.

**Purpose:** This PIA was conducted because PII is collected during security threat assessments.

**DHS/S&T/PIA-008(c)** ***Facial Recognition Data Collection Project Update (September 16, 2013)***
**Background:** The Department of Homeland Security Science and Technology Directorate (S&T) Resilient Systems Division has funded Pacific Northwest National Laboratory to perform a face video data collection at the at the Toyota Center in Kennewick, Washington. The S&T Resilient Systems Division is collecting facial video data to test and evaluate facial recognition software. The actual identities of the volunteer participants will not be disclosed to any federal government agencies, and the goal of the project is to determine the accuracy of facial recognition software.

**Purpose:** S&T updated this PIA to address the privacy risks associated with facial video data collection and facial recognition software testing, and how S&T mitigates those risks.

**DHS/USCIS/PIA-030(b)** ***E-Verify Self Check (September 6, 2013)***
**Background:** E-Verify Self Check is an online service that allows U.S. employees to check their employment eligibility in the United States before beginning a new job. E-Verify was mandated by the *Illegal Immigration Reform and Immigrant Responsibility Act of 1996* (IIRIRA), which requires that the E-Verify system be designed and operated to maximize reliability and ease of use. Therefore, DHS developed E-Verify Self Check.

The E-Verify Self Check service is voluntary and available to any individual who wants to check his own work authorization status prior to employment, and facilitate correction of potential errors in federal databases that provide inputs into the E-Verify process. When an individual uses the E-Verify Self Check service, he will be notified that either; 1) his information matched the information contained in federal databases and would be deemed work-authorized, or, 2) his information was not matched to information contained in federal databases which would be considered a "mismatch." If the information was a mismatch, he will be given instructions on where and how to correct his records.

**Purpose:** The system provides a vehicle for individuals to proactively check work authorization status prior to the employer conducting the E-Verify query. This PIA was conducted because E-Verify Self Check collects and uses PII.

## B. System of Records Notices

As of November 30, 2013, 98 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.

During the reporting period the DHS Privacy Office published five SORNs and one Notice of Proposed Rulemaking (NPRM). Three SORNs are summarized below, and a hyperlink to the *Federal Register Notice* is included for each document listed. All DHS SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act Exemptions are available on the DHS Privacy Office website, www.dhs.gov/privacy.

**DHS/CBP-019 - Air and Marine Operations Surveillance (AMOSS) System of Records**
This is a new system of records that allows CBP to collect and maintain records on publicly available aircraft and airport data provided by the Federal Aviation Administration, requests from law enforcement about suspects, tips from the public, and recordings of event and operations data in a watch log or event tracking log. DHS issued a NPRM in connection with this SORN to exempt this system of records from certain provisions of the Privacy Act.

**DHS/TSA-019 Secure Flight System of Records**
This system of records allows TSA to collect and maintain records on aviation passengers and certain non-travelers to screen such individuals before they access airport sterile areas or board aircraft in order to identify and prevent a threat to aviation security or the lives of passengers and others. DHS/TSA reissued this system of records notice to update the categories of records to include whether a passenger will receive expedited, standard, or enhanced screening. The primary impact of this change will be the identification of additional passengers who are eligible for expedited screening at participating airport security checkpoints.

**DHS/USCIS-008 - Refugee Access Verification Unit System of Records**
This system of records allows the U.S. Citizenship and Immigration Services (USCIS) to collect information to verify claimed relationships between anchor relatives in the United States and their overseas family members seeking access to the U.S. Refugee Admissions Program under the Priority 3 Family Reunification Program. Eligible anchor relatives who were admitted to the United States as refugees or granted asylum in the United States may file an Affidavit of Relationship for qualifying overseas family members (spouses, unmarried children under age 21, and/or parents) to seek access to the U.S. Refugee Admission Program for their family members under the Priority 3 program. USCIS updated and reissued this system of records notice to include: (1) an updated system location; (2) updated categories of records; (3) updated routine uses; (4) a proposed retention schedule; (5) updated data elements used to retrieve records; and (6) updated sources of records. Additionally, this updated SORN includes non-substantive changes to simplify the formatting and text of the previously published notice.

## 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 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 and Memoranda of Agreement.

During the reporting period, the Office initiated a PCR for CBP's Analytical Framework for Intelligence (AFI), as called for in the AFI PIA dated June 1, 2012. AFI enhances DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs and immigration laws, and other laws enforced by DHS at the border. The PCR was still in progress when the reporting period ended.

PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under review. Public PCR reports are available on the DHS Privacy Office website, www.dhs.gov/privacy, under "Investigations and Compliance Reviews."

# IV. ADVICE AND RESPONSES

## A. Privacy Training and Awareness

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

### *Mandatory Training*

122,540 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*

1,091 DHS personnel attended instructor-led privacy training courses, primarily privacy training for new employees:

- The DHS Privacy Office provides privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees.
    - Many of the Component Privacy Officers[16] also offer privacy training for new employees when they onboard.
- The DHS Privacy Office provides monthly privacy training as part of the two-day course, *DHS 101*, which is required for all new and existing headquarters staff.

### *Miscellaneous Training*

- **"DHS 201" International Attaché Training:** The Department's "DHS 201" training module is a week-long course designed to prepare DHS employees who serve as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. The DHS Privacy Office provides an international privacy policy module to raise awareness among new attachés of the potential impact of global privacy policies. The Office trained 42 participants in two training sessions during the reporting period.

- **DHS Security Specialist Certification Course**: The Office provides privacy training each month to participants of the week-long Security Specialist Training Certification Program. During the reporting period, 60 staff from all DHS Components were trained.

[16] 10 DHS offices and components have a Privacy Officer.

# B. DHS Privacy Office Awareness & Outreach

## *Meetings & Events*

- Data Privacy & Integrity Advisory Committee (DPIAC) Meeting – On September 12, 2013, the Privacy Office held a public meeting of the DPIAC. Committee members agreed on a draft recommendation report regarding privacy considerations in the Department's use of live data[17] for training, testing, or research. The Committee agreed that there are occasions when the use of live data containing personal information in research, testing, or training can be justified. There were twelve specific recommendations, including the use of a rigorous privacy risk analysis process to allow privacy officers to determine the necessity and the privacy risks implicated by such a proposed use. The final report will be submitted to the Secretary and the Chief Privacy Officer for their consideration.
- Senate Homeland Security and Governmental Affairs Committee (HSGAC) Briefing – On September 24, 2013, the Privacy Office, in conjunction with CBP, the Common Vetting Task Force, Office of the Chief Information Officer, and Office of Intelligence & Analysis, gave an unclassified briefing to HSGAC staff members on the DHS Data Framework, specifically the tests for Common Entity Index Prototype, Cerberus, and Neptune.
- Senate Select Committee on Intelligence (SSCI) Briefing – On October 4, 2013, the Privacy Office, in conjunction with CBP, the Common Vetting Task Force, Office of the Chief Information Officer, and Office of Intelligence & Analysis, gave an unclassified briefing to the SSCI staff members on the DHS Data Framework, specifically the tests for Common Entity Index Prototype, Cerberus, and Neptune.
- The Lemelson Center for the Study of Invention and Innovation, Smithsonian National Museum of American History Symposium – On October 25, 2013, the Deputy Chief Privacy Officer participated in a symposium titled, "Perspectives on the Surveillance Society."
- Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce Hearing – On November 19, 2013, the Chief Privacy Officer testified at a hearing titled "Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions Within the Federal Workforce." She reviewed the Privacy Office's privacy compliance process, including PIAs and PCRs.
- DPIAC Cybersecurity Subcommittee Meeting – On November 25, 2013, the Privacy Office and the National Protection and Programs Directorate (NPPD) co-hosted a meeting of the DPIAC's Cybersecurity Subcommittee. The Subcommittee is comprised of representatives from the full Committee and additional subject matter experts from the privacy and civil liberties community. DHS sponsors TS/SCI clearances for the subcommittee members and provides classified and unclassified briefings to the members on DHS cyber operations. During this meeting, NPPD briefed members on the Einstein 3 Accelerated and Enhanced Cybersecurity Services programs, as well as on the operations of the National Cybersecurity and Communications Integration Center; the United States Secret Service (USSS) briefed members on recent operations.

[17] Certain DHS components use or plan to use personally identifiable information (PII) collected for operational use (live data) for training purposes, for testing new or updated systems, or for research.

# C. Component Privacy Office Awareness & Outreach

## *National Protection and Programs Directorate*

- Trained Information Technology (IT) contractors supporting OBIM's systems operations on privacy awareness and the prevention of privacy incidents on October 16, 22, and 24.

- Provided privacy and acquisitions training to the Office of Infrastructure Protection Contracting Officer Representatives on November 6, 2013. The training was provided to 28 participants on how to apply provisions for required training for contractors, breach and privacy compliance to Statements of Work and other supporting contract documents.

- Released an edition of the *Privacy Update*, NPPD's quarterly privacy awareness publication, to keep employees abreast of privacy news and emerging issues surrounding technology. In this issue, NPPD highlighted National Cybersecurity Awareness Month, United States Computer Emergency Readiness Team (US-CERT)'s outreach efforts via Twitter, and privacy concerns surrounding Apple's iPhone 5S release. NPPD also issued a reminder on incorporating privacy into acquisitions vehicles and holding contractors accountable for safeguarding Sensitive PII.

- Published three privacy tips in OBIM's newsletter and SharePoint site on the following topics: 1) encryption of Sensitive PII; 2) using DHS email accounts and not personal/corporate accounts to prevent privacy incidents; and 3) safe online shopping during the holidays.

## *Science and Technology Directorate*

- Presented on S&T's uses of unmanned aircraft and the Robotic Aircraft for Public Safety Test and Evaluation Project at the DPIAC meeting on September 12.

- Presented at the Biometrics Consortium Conference on perceptions of privacy in relation to uses of biometrics on September 19.

## *United States Citizenship and Immigration Services*

- Developed and conducted a privacy briefing entitled "*Privacy Program Overview and Priorities*," to Southeast Region's District Directors and Field Office Directors. This briefing provided an overview of the USCIS Office of Privacy's policies, procedures, and processes, along with the purpose and function of the Regional Privacy Program and how the Southeast Regional Privacy Officer can assist leadership in ensuring compliance with privacy regulations, policies and procedures.

- Developed a specialized training module entitled "*Privacy Compliance Boot Camp*" to provide guidance on how to complete privacy compliance documentation, including PTAs, PIAs, SORNs and Privacy Act (e)(3) statements, to system owners, program managers, information system security managers, and to all individuals who may be responsible for reviewing and/or developing privacy compliance documentation.

- Conducted and completed 17 site visits and risk assessments of various USCIS facilities. Provided insight and recommendations to leadership on findings/privacy risks, and how to improve privacy protections and awareness throughout each region.

- Hosted a new *"Town Hall Forum"* for the Orlando Field Office so the Southeast Regional Privacy Officer could address any questions from employees and contractors on to how to determine a privacy incident, report and mitigate a privacy incident, prevent a privacy incident, etc. The forum also gave employees the opportunity to share their thoughts and provide feedback on privacy policies and procedures relating to privacy incidents.

- Published a privacy awareness/education article entitled "*Protecting PII on your Shared Drives*" in the California Service Center's monthly newsletter. This article addressed the "*Dos*" and "*Don'ts*" when safeguarding PII and Sensitive PII on USCIS shared drives.

- Published the USCIS Office of Privacy fourth quarter newsletter entitled "*Privacy Chronicles*," which focused on promoting privacy awareness across USCIS through our *Third Annual Privacy Awareness Day*. It also focused on how it is important, as an agency, that employees and contractors understand their responsibility to promote transparency while safeguarding PII that has been entrusted to the agency through adherence to USCIS privacy policies, partaking in privacy training initiatives, and through initiatives such as the USCIS Drive Clean-up Day and USCIS PIAs.

- Published multiple Privacy Tips on the USCIS intranet, highlighting topics that focused on the appropriate use, access, sharing, and disposing of PII, and how to effectively report a privacy incident.

### *United States Immigration and Customs Enforcement*

- Presented best practices on how to properly handle Sensitive PII and prevent privacy incidents at the ICE Office of Professional Responsibility, Office of Detention Oversight, New Employee Orientation Training on September 25.

- Provided content on privacy and social media to 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*. U.S. citizens, Legal Permanent Residents, visitors, and aliens submit complaints.[18]

**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[19] | In Progress (Current Period) | In Progress (Prior Periods) |
| **Process & Procedure** | 0 | 0 | 0 | 4 |
| **Redress** | 0 | 0 | 0 | 0 |
| **Operational** | 960 | 896 | 244 | 10 |
| **Referred** | 4 | 4 | 0 | 0 |
| ***Total*** | ***964*** | ***900*** | ***244*** | ***14*** |

.

DHS separates 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 inspection at the border or screening at airports.[20]
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.

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

[19] These totals include complaints opened and closed during this reporting period, and complaints opened in prior reporting periods but closed during this reporting period.

[20] 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.

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 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:

## *United States Customs and Border Protection*

**Complaint:** The CBP INFO Center was contacted by a complainant who reported that after passing through Exit Control upon arrival in the United States, a CBP officer ran after her and asked for her passport. When the complainant provided it, the CBP officer purportedly turned to a plain-clothed colleague to ask a question about the complainant's passport. The CBP officer returned the passport after discussion with his colleague but offered no explanation as to why the traveler was stopped or why her passport was shared with the plain-clothed colleague. The complainant was embarrassed and outraged over the incident, and felt her PII had been compromised.

***Disposition*:** The CBP INFO Center referred this complaint to the District Field Officer (DFO) for investigation, review, and response back to the complainant. The DFO contacted the complainant and explained that at the time of her arrival at Exit Control, CBP was conducting an enforcement operation in conjunction with another federal agency; the plain-clothed individual accompanying the CBP officer was present because of that operation. The DFO provided that sometimes matters have to be handled quickly and without complete explanation. The DFO gave the complainant her contact information if there were any problems in the future. The complainant understood and was satisfied with the DFO explanation.

**Complaint:** A complainant who is a member of Global Entry (GE), a CBP Trusted Traveler Program (TTP), contacted the CBP INFO Center because the PASSID number, assigned as a unique identifier, was not appearing on boarding passes issued to him by a certain airline carrier. When the complainant inquired with this carrier, it was determined that the name on the GE card did not match the name on the boarding pass and that the GE card needed to be corrected. The complainant then contacted the CBP INFO Center to correct the erroneous GE card, and his non-selection for the Pre Check program as a result of this error was also to be re-examined.

***Disposition*:** The CBP INFO Center obtained a copy of the complainant's Global Entry card and the correct full name, date of birth, and passport number. The CBP INFO Center then referred the complainant to the Trusted Traveler Program at CBP Headquarters, where the corrected information was confirmed and his biographic information in the Global Entry account was updated. The CBP INFO Center then reached out to the complainant to advise that the Global Entry card had been corrected and a new card was issued and would be received in the mail.

# VI. CONCLUSION

As required by the 9/11 Commission Act, this quarterly report summarizes the DHS Privacy Office's activities from September 1 – November 30, 2013. The DHS Privacy Office will continue to work with the Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.