



Department of Homeland Security

Privacy Office

Third Quarter Fiscal Year 2012 Report to Congress

August 2012



Homeland
Security

I. FOREWORD

August 14, 2012

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *Third Quarter Fiscal Year 2012 Report to Congress*. This quarterly report includes activities from March 1, 2012 – May 31, 2012,¹ and reflects the work of my predecessor, Chief Privacy Officer Mary Ellen Callahan, and the DHS Privacy Office staff.²



Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*³ (*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.⁴ 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*,⁵ the *Freedom of Information Act*⁶ (FOIA), the *E-Government Act of 2002*,⁷ and the numerous 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 periods established for reporting under *The Federal Information Security Management Act of 2002* (“FISMA”, [44 U.S.C. § 3541](#), *et seq.*) rather than the fiscal year.

² Former CPO Mary Ellen Callahan recently left the DHS Privacy Office, after 40 months of service to DHS.

³ 42 U.S.C. §2000ee-1(f).

⁴ 6 U.S.C. §142.

⁵ 5 U.S.C. §552a.

⁶ 5 U.S.C. §552.

⁷ Pub. L. 107-347, § 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 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 202-343-1717 or privacy@dhs.gov. This report and other information about the Office are available on our website, listed below.

Sincerely,



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



**DHS PRIVACY OFFICE
THIRD QUARTER FISCAL YEAR 2012
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. Systems of Record Notices	10
	C. Privacy Compliance Reviews	11
	D. Other Privacy Reviews	13
IV.	ADVICE AND RESPONSES.....	14
	A. Privacy Training and Awareness	14
	B. DHS Privacy Office Awareness & Outreach	15
	C. Component Privacy Office Awareness & Outreach	16
V.	PRIVACY COMPLAINTS AND DISPOSITIONS.....	18
VI.	CONCLUSION	21

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 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) required under the *E-Government Act of 2002* and the *Homeland Security Act of 2002*,⁸ as amended, and by DHS policy;
3. System of Records Notices (SORN) as required under the *Privacy Act*⁹ and associated *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 Report as required by Section 804 of the *9/11 Commission Act*;¹³
7. Privacy Compliance Reviews;
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.

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.

**Reviews Conducted During
Third Quarter Fiscal Year 2012**

Review Type	# of Reviews
Privacy Threshold Analyses	233
Privacy Impact Assessments	15
System of Records Notices and Associated <i>Privacy Act</i> Exemptions	2
<i>Privacy Act</i> (e)(3) Statements	9
Computer Matching Agreements	1
Data Mining Reports	0
Privacy Compliance Reviews	2
Privacy Reviews of IT and Program Budget Requests	0
Other Privacy Reviews	2
<i>Total Reviews</i>	264

A. Privacy Impact Assessments

The Privacy Impact Assessment (PIA) process is one of the key mechanisms used to assure that the Department's programs and technologies sustain, and do not erode, privacy protections for DHS' use, collection, and disclosure of PII. As of May 31, 2012, 81 percent of the Department's Federal Information Security Management Act (FISMA) systems requiring a PIA were subject to a PIA. Due to additional systems coming online, this represents no change from the 81 percent subject to a PIA during the prior reporting period.

In addition to completing PIAs for systems that are not currently subject to a PIA, the Department has implemented a triennial review program for existing PIAs to assess and confirm that the systems covered under those PIAs are still operating within the originally published parameters. As these triennial reviews are completed, previously-published PIAs will be updated to inform the public that a review has been completed for the affected systems.

The Department published 15 PIAs during this reporting period and five of them are summarized below. 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 lower-case letter after the original PIA number.*

DHS/USSS/PIA-009 - Field Investigative Reporting System (FIRS)

Background: The U.S. Secret Service (Secret Service) has created the Field Investigative Reporting System (FIRS). FIRS consist of seven applications for the reporting of law enforcement activities within the Secret Service's jurisdiction, such as investigating counterfeiting and electronic crimes.

Purpose: The Secret Service conducted this PIA because FIRS is a new system that contains the PII of subjects of criminal investigations. *(March 7, 2012)*

DHS/TSA/PIA-018(e) - Secure Flight Program Update

Background: The Transportation Security Administration (TSA) Secure Flight program screens aviation passengers and certain non-travelers before they access airport sterile areas or board aircraft. This screening compares these individuals to the No Fly and Selectee portions of the consolidated and integrated terrorist watch list, against other watch lists maintained by the Federal Government when warranted by security considerations, and against a list of passengers who have been assigned a unique redress number by the DHS Traveler Redress Inquiry Program. Secure Flight allows for DHS/TSA to create a Known Traveler program in order to expedite screening of low risk travelers.

Purpose: This updated PIA reflects the establishment of the TSA Pre✓™ program and its interaction with Secure Flight. TSA Pre✓™ will incorporate the proof of concept Known Traveler program identified in the August 2011 PIA Update in which TSA recognizes existing U.S. Customs and Border Protection (CBP) Trusted Traveler programs and eligible members of the U.S. Armed Forces for expedited screening (while reserving the right to incorporate random enhanced screening protocols). TSA is exploring the feasibility of expanding the Known Traveler program beyond these populations to include groups such as certain active security clearance holders, aviation workers and other transportation sector populations for whom TSA performs a security threat assessment, and other populations. This PIA will be updated as TSA incorporates new Known Traveler populations into the Secure Flight program. *(April 13, 2012)*

DHS/USCIS/PIA-041 – ELIS-1 Temporary Accounts and Draft Benefit Requests

DHS/USCIS/PIA-042 – ELIS-2 Account and Case Management

DHS/USCIS/PIA-043 – ELIS-3 Automated Background Functions

Background: U.S. Citizenship and Immigration Services (USCIS) is transforming its operations by creating a new electronic environment known as the USCIS Electronic Immigration System (USCIS ELIS), which allows individuals requesting a USCIS benefit to register online and submit certain benefit requests through the online system. This system will improve customer service; increase efficiency for processing benefits; better identify potential national security concerns, criminality, and fraud; and create improved access controls and better auditing capabilities. The electronic environment is divided into three distinct processes: (1) Temporary Account and Draft Benefit Requests; (2) Account and Case Management; and (3) Automated Background Functions.

Purpose: One PIA addresses the Temporary Account and Draft Benefit Requests process by describing how Applicants or their Representatives can create a temporary account, draft a benefit request, and submit or abandon that request. Another PIA addresses the Account and Case Management process by describing how USCIS ELIS uses information provided on initial and subsequent benefit requests and subsequent collections to create or update USCIS ELIS accounts; gather any missing information; manage workflow; assist USCIS in making a benefit determination; and provide a repository of data to assist with future benefit requests. The third PIA addresses the Automated Background Functions process, which includes the actions USCIS ELIS takes to ensure that serious or complex cases receive additional scrutiny by detecting duplicate and related accounts and identifying potential national security concerns, criminality, and fraud. (*May 16, 2012*)

B. System of Records Notices

As of May 31, 2012, 96 percent of the Department's FISMA systems that require a System of Records Notice (SORN) were covered by 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.

All DHS SORNs and Final Rules for Privacy Act Exemptions can be found on our website, www.dhs.gov/privacy.

During this reporting period, DHS published one SORN and one Final Rule for Privacy Act Exemptions:

DHS/CBP-006 Automated Targeting System [ATS] System of Records Notice

This SORN was updated to inform the public that CBP expanded the categories of individuals, categories of records, and sources of records stored in ATS to reflect data that it must ingest for performance purposes. CBP had previously exempted portions of ATS from the notification, access, amendment, and public accounting provisions of the *Privacy Act* because it is a law enforcement system. CBP, however, will consider each request for access to records maintained in ATS to determine whether or not information may be released.

CBP further noted that despite the exemption taken on this system of records, they are providing access and amendment rights to Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, Importer Security Filing (10+2 documentation) information, and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the *Privacy Act*. (May 22, 2012)

C. Privacy Compliance Reviews

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

During this reporting period, the DHS Privacy Office conducted and published the results of two PCRs. Reports on the results of PCRs can be found on our website www.dhs.gov/privacy.

DHS Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue, and DHS Use of Unidirectional Social Media Applications Communications and Outreach

DHS utilizes social media for communications, public affairs, and outreach purposes, and has an official presence on many of the major social media platforms such as Facebook, Twitter, and YouTube. To ensure that DHS' use of social media for communications and public outreach adheres to privacy requirements, DHS developed two Department-wide PIAs: one PIA for the Department's use of social networking interactions and applications; and another PIA for the Department's use of unidirectional social media.¹⁴

The DHS Privacy Office conducted this PCR to (1) determine whether selected DHS social media uses listed in the DHS-wide social media PIA appendices continue to meet the requirements as described in the PIAs and (2) to determine if the appendices of the DHS-wide social media PIAs reflect an accurate accounting of DHS users.

National Operations Center Publicly Available Social Media Monitoring and Situational Awareness Initiative

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), has a statutory responsibility to: (1) provide situational awareness and establish a common operating picture for the Federal Government, and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other man-made disaster; and (2) to ensure that critical terrorism and disaster-related information reaches government decision makers.¹⁵ Traditional media sources, and more recently social media sources, such as Twitter, Facebook, and blogs, provide public reports on breaking events with a potential nexus to homeland security. By examining open source traditional and social media information, comparing it with many other sources of information, and including it where appropriate in NOC reports, the NOC can provide a more comprehensive picture of new or evolving events.

¹⁴ See DHS/ALL/PIA-031 Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue (September 16, 2010) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_socialnetworkinginteractions.pdf and DHS/ALL/PIA-036 Use of Unidirectional Social Media Applications (March 8, 2011) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_unidirectionalsocialmedia.pdf.

¹⁵ Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).

PCRs are a key aspect of the layered privacy safeguards built into this initiative to ensure protections described in the PIAs are followed. Accordingly, the DHS Privacy Office conducted this bi-annual PCR to: (1) assess compliance with the January 2011 PIA Update and February 2011 SORN;¹⁶ and (2) review and update, as appropriate, the 2011 Analyst's Desktop Binder and Standard Operating Procedures (SOPs) to ensure they accurately reflect the scope of the initiative. The DHS Privacy Office found NOC to be in compliance with the privacy requirements identified in the January 2011 PIA Update and the February 2011 SORN, and made three recommendations to improve the NOC's ability to demonstrate its continued compliance. The NOC has already taken steps to address all of these recommendations. (*May 3, 2012*)

¹⁶ See DHS/OPS/PIA-004(d) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update (January 6, 2011) available at: http://www.dhs.gov/files/publications/gc_1281732303362.shtm#3

D. Other Privacy Reviews

The DHS Privacy Office also conducts other privacy reviews, such as implementation reviews for information sharing agreements.

During the reporting period, the DHS Privacy Office engaged in the following two quarterly reviews:

- Implementation aspects of the Automated Targeting System (ATS). ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. DHS identifies travel patterns that may indicate illicit activities and develops targeting rules from intelligence information that are incorporated into ATS. These rules are reviewed quarterly by CBP, the DHS Privacy Officer, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel to determine if the rules are appropriate, relevant and effective; and
- Results of several information sharing agreements with the National Counterterrorism Center (NCTC) in conjunction with the Office for Civil Rights and Civil Liberties, the Office of Intelligence and Analysis, and the Office of the General Counsel.

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

Mandatory Training

43,560 DHS personnel completed the mandatory computer-assisted privacy training course, Culture of Privacy Awareness. This course must be taken by all new personnel when they join the Department, and annually thereafter.

New Employee Training

2,410 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 Officers¹⁷ 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 this reporting period, 149 people were trained in 7 sessions at 7 fusion centers.*
- The DHS Privacy Office provides training to I&A intelligence professionals selected for assignment to fusion centers, as required under Section 511 of the *9/11 Commission Act*.¹⁸
 - *During this reporting period, no I&A intelligence professionals were trained on privacy policy because no new analysts were assigned.*

Nationwide Suspicious Activity Reporting Initiative

- The DHS Privacy Office also provides training to Suspicious Activity Reporting (SAR) analysts.
 - *During this reporting period, 29 analysts were trained on privacy issues related to suspicious activity reporting.*

¹⁷ Each of the 10 sub-Components that comprise the Department has a Privacy Officer.

¹⁸ Pub. L. 110-53, §511, 6 U.S.C. §101 note.

B. DHS Privacy Office Awareness & Outreach

Publications

Handbook for Safeguarding Sensitive Personally Identifiable Information – In March, the Privacy Office published a completely revised version of this Handbook, which sets minimum standards for how Department personnel should handle Sensitive PII in paper and electronic form during their everyday work activities. The Handbook can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

Outreach

DHS Privacy Office Speaker Series – On April 18, the DHS Privacy Office held the latest event in its Speaker Series, open to all Federal Government employees. Two experts discussed the many applications for virtual worlds in the Federal Government, and their impact on privacy.

Meetings & Events

- National Fusion Center Training Event – From April 2 to 6, the Senior Advisor for Information Sharing and the Senior Privacy Analyst for Intelligence participated as panelists on the *Implementing Privacy Policy Requirements* panel at the National Fusion Center Training Event in Phoenix, Arizona.
- Department of Treasury Records and Information Management Month's Panel on International Privacy – On April 17, the Chief Privacy Officer spoke on a panel regarding international privacy as part of the Department of Treasury's Records and Information Management Month.
- Department of Veterans Affairs Workshop – On April 18, the Associate Director for Privacy Compliance provided a privacy compliance overview at this workshop, as part of their "VA Privacy Speaker Series."
- USCIS Privacy Awareness Week – On April 23, the Chief Privacy Officer gave a keynote address to kick off the USCIS Privacy Awareness Week.
- Government Accountability Office (GAO) Conference on Civil Unmanned Airspace Systems – On April 24, the Associate Director for Privacy Compliance attended this conference to address questions on potential impacts on information privacy, civil rights and civil liberties by government operated unmanned airspace systems.
- Privacy Training & Awareness Best Practices Workshop - On May 9, the Privacy Office, under the aegis of the Federal Chief Information Officer Privacy Committee, sponsored a two hour workshop attended by 120 people from numerous executive branch agencies. The DHS Associate Director of Communications and Training and the Acting Chief Privacy Officer at the Federal Trade Commission co-led the workshop, which featured compelling ways to create a culture of privacy within an agency.
- Chief Security Office Privacy Presentation – On May 17, the Associate Director of Communications and Training presented methods to safeguard Sensitive PII to 200 DHS Chief Security Office staff at a special All Hands Meeting in Washington, D. C.

C. Component Privacy Office Awareness & Outreach

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

- The ICE Privacy Officer presented at the Homeland Security Investigations Intelligence Conference in New Orleans on May 30.
- The Privacy Office distributed a tip on how to properly handle and safeguard Sensitive PII to all ICE employees via *ICE Info* on May 2.

Intelligence & Analysis (I&A) Privacy Office--Headquarters

- The I&A Privacy Officer briefed 44 personnel newly assigned to I&A on I&A's SORNs, PIAs, PTAs and how to safeguard PII.
- The Privacy Office published an I&A Policy Directive on the handling of Sensitive PII.

National Protection and Programs Directorate (NPPD) Office of Privacy

- Office of Privacy staff provided specialized training to the Office of Infrastructure Protection, Infrastructure Security Compliance Division, on the intersection between the Paperwork Reduction Act and privacy compliance processes.
- Office of Privacy staff provided specialized training to the US-CERT Senior Watch Officers to highlight privacy equities in cyber security.
- Office of Privacy staff launched a pilot for the newly recorded NPPD Privacy 101 Training on Homeland Security Information Network Connect. This training is designed as an electronic educational resource for employees and contractors who are either located off-site or work alternate schedules and may not be able to attend in-person training.
- Office of Privacy staff rolled out a new *E-mail Best Practices Guide* to educate employees on best practices for emailing Sensitive PII.

United States Citizenship and Immigration Services (USCIS) Privacy Office

- USCIS Privacy Officer conducted specialized training for the Field Office Directors on privacy and how it relates to USCIS, and on their roles and responsibility to ensure that privacy has been incorporated into the field offices' standard operating procedures by ensuring that employees and contractors under their leadership are aware of their responsibility to safeguard PII from unauthorized access, use, sharing and distribution. The training occurred on March 29.
- USCIS privacy staff served as presenters at the *Mission Support Training* in Burlington, Vermont, which provides mission-specific cross training to Mission Support Specialists on all USCIS Programs. The Office of Privacy participated in this training by conducting mandatory privacy awareness training. 32 Mission Support Specialists were trained in privacy policy. This training occurs quarterly, and the most recent event was held on March 29.

- From April 23 to 27, the Office of Privacy, in partnership with the Verification Division's Privacy Branch, developed and hosted its *Second Annual Privacy Awareness Week*, which featured: (1) the first agency-wide *National Clean-up Day* where employees reviewed and disposed of records that were no longer needed for business purposes; and (2) instructor-led privacy awareness training throughout the week.

United States Coast Guard (USCG) Privacy Office

- The USCG Privacy Officer hosted three privacy awareness presentations for 400 human resources staff at the USCG facility located at Ballston, Virginia on April 10.
- The USCG Privacy Officer sent a message USCG-wide to remind the fleet of the importance of safeguarding PII on May 9. This message included a definition of PII, examples of USCG privacy incidents, and privacy policies.

United States Secret Service (USSS) Privacy Office

- Privacy Office staff provided training on safeguarding PII and how to report privacy incidents to all administrative officers employed at headquarters and field offices at the Secret Service's Rowley Training Center.
- Privacy Office staff issued an official message to all USSS employees on the importance of safeguarding PII, reporting privacy incidents, and reminded employees of a dedicated phone line and email account within the FOIA/Privacy Program for Privacy and FOIA related inquiries and/or comments.

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.¹⁹

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	4	0	3
Redress	3	3	0	1
Operational	329	328	18	11
Referred	1	1	0	0
Total	337	336	18	15

*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 and/or correction of PII, and appropriate redress of such issues.
Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.²⁰
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.

¹⁹ See *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*.

²⁰This 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.

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 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 disposition:

National Protection Programs Directorate (NPPD)

Complaint: NPPD's U. S. Visitor and Immigrant State Indicator Technology Program (U. S. – VISIT) received a redress request from the ICE attaché in London regarding a couple that was experiencing difficulties at the ports of entry during their visits to the United States. In the request, the couple described inconveniences endured when visiting the United States, including their most recent visit in which the wife spent four hours in secondary inspection.

Disposition: NPPD researched the case and found that, during one of their earlier visits, the husband's biometrics and photograph had been inadvertently attached to the wife's record in the Automated Biometric Identification System (IDENT). This mismatch resulted in the couple being referred to secondary inspection in subsequent visits. NPPD reviewed and corrected the record in the IDENT system and anticipates this will prevent the couple from being referred to secondary inspection in the future.

Transportation Security Administration (TSA)

Complaint: The TSA Privacy Office received a complaint from an employee stating that management allowed a co-worker of the same pay grade and position to participate in the employee's performance evaluation review session.

Disposition: The TSA Privacy Office contacted the Assistant Federal Security Director at the airport in question and confirmed that the co-worker served in the role of "recorder", or note taker, with an official need to know the information. The TSA Privacy Office reviewed the details associated with this incident and contacted the Office of Human Capital to review their policies and practices. The TSA Privacy Office advised the individual that based on current policy, no Privacy Act violation existed because the co-worker served as a "recorder" of the performance evaluation at the request of management.

U.S. Customs and Border Protection (CBP)

Complaint: The CBP INFO Center received a complaint from a female traveler who expressed concern about how CBP officers treated her during processing at her Port of Entry. The complainant maintains that the CBP officer who questioned her during secondary inspection was “unprofessional” and asked her questions that were “very personal and intrusive.” The complainant further noted that she had to wait a long time for the process and felt that the CBP officer was intentionally delaying the process because she was a woman traveling alone.

Disposition: Pursuant to a thorough review of this incident, the Port Director sent a letter to the complainant, apologizing for any rude or unprofessional behavior of the CBP officers but noted that the officers “acted within the scope of their authority.” The letter further noted that the Port Director has mandated additional training on the handling of travelers. Counseling is also being provided on this topic during officer meetings.

U. S. Immigration and Customs Enforcement (ICE)

Complaint: An ICE employee submitted a privacy complaint to the ICE Privacy Office and the ICE Office of Professional Responsibility (OPR), alleging that a non-supervisory individual improperly accessed and disclosed promotion information about the employee. The employee stated that the non-supervisory individual congratulated her on a promotion before it was made official. The employee also stated that the non-supervisory individual was not the Human Resources liaison for her program office, and she was concerned that the individual was provided improper access to her personnel actions.

Disposition: OPR referred the complaint to program office management for additional review and investigation. The program office found that the non-supervisory individual acted within her official capacity and that congratulating an employee about a promotion did not constitute improper disclosure of PII. The ICE Privacy Office concurred with this finding. The program office responded to the complainant, and the complaint was closed as “no privacy violation.”

VI. CONCLUSION

As required by the *9/11 Commission Act*, this quarterly report provides a summary of the DHS Privacy Office's activities from March 1, 2012 – May 31, 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.