Department of Homeland Security
Report of the Chief Privacy Officer Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007

December 1, 2008

Introduction

The Department of Homeland Security (DHS) Chief Privacy Officer is the first statutorily mandated Chief Privacy Officer in the Federal government. The mission of the Privacy Office is to sustain privacy protections and to promote transparency of government operations while achieving the mission of the Department. Within the Department, the Privacy Officer implements Section 222 of the Homeland Security Act[1], the Privacy Act of 1974[2], the Freedom of Information Act[3], the E-Government Act of 2002[4], and the numerous laws, Executive Orders, court decisions and DHS policies that protect the collection, use, and disclosure of personally identifiable information collected, used, maintained, or disseminated by DHS.

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, established additional privacy and civil liberties requirements for DHS. Pursuant to the requirements of Section 803, the Privacy Office is providing its 1st quarter report for fiscal year 2009.[5] This report in large part covers the period of September 1, 2008 to November 30, 2008. The DHS Office for Civil Rights and Civil Liberties will provide a separate report regarding civil liberties.

As DHS continues to review the complaints and responses, DHS may modify the categories over time to reflect the types of complaints received.

---

[1] 6 U.S.C. § 101 *et seq.*
[2] 5 U.S.C. § 552a *et seq.*, as amended.
[3] 5 U.S.C. § 552.
[4] 44 U.S.C. § 3501.
[5] The reporting period matches the existing reporting period required for Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) IT Security and Privacy reporting.

1st Quarter 2009 Section 803 Report
September 1, 2008 – November 30, 2008

Reviews:

Type of Review	Number of Reviews
Privacy Threshold Analyses	47
Privacy Impact Assessments	23
System of Records Notices and associated Privacy Act Exemptions	41
Privacy Act (e)(3) Statements	2
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Protection Reviews of IT and Program Budget requests	13
Total Reviews for Q1FY09	*126*

For additional descriptions of the above, please see Appendix I.

Advice & Responses:

During the reporting period, DHS released the following guidance related to privacy:

1. The DHS Privacy Office issued the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, found at www.dhs.gov/privacy under "Privacy Policy Guidance and Reports".
2. The U. S. Coast Guard (USCG), a component of DHS, continued to engage with programs regarding Privacy Compliance by reviewing all new or updated to existing directives. To ensure compliance, safeguarding measures and incident handling directions are incorporated in all documents/publications relating to PII. During this period the CG Privacy Office reviewed 30 directives and 5 General Messages (ALCOASTS) and 2 Operating Facility Change Orders (OFCO).
3. To promote awareness and safeguarding PII, the USCG Privacy Office met with 25 office move coordinators at CG Headquarters during one of their monthly meetings. Discussion points included: (a) Conducting a walkthrough of spaces in the early planning stages of the move to identify privacy concerns and issues; (b) Providing guidance to personnel on the importance of safeguarding PII during all phases of the move; (c) Using the move as an

opportunity to purge files, ensuring continued retention or destruction of records is in accordance with CG instructions and Federal law.

During the reporting period, DHS conducted the following training:

1. DHS personnel and contractors took classroom-based privacy training courses in 336 instances.
2. DHS personnel and contractors took computer-assisted privacy training courses in 5,594 instances.

The Transportation Security Administration (TSA), a component of the Department of Homeland Security, issued Broadcast Message on Limiting Information Access to Official Purposes. The TSA Privacy Office transformed the TSA Privacy Intranet page into a comprehensive I-Share site.

The USCG Privacy Officer delivered a brief presentation to 12 course/curriculum designers on the importance of ensuring their final products do not contain PII. Information passed addressed blurring out names/name tags on vides, prohibiting the use of any PII on forms/examples and employing appropriate warning banners when applicable.

US-VISIT, a component of the Department of Homeland Security, conducted the US-VISIT Privacy Awareness Week, on October 20-24, 2008. The all-hands kick off had a very successful turn-out event, the Chief Privacy Officer of the Federal Trade Commission spoke about protecting privacy. Two brown bag events were also held during US-VISIT Privacy Awareness Week with guest speakers. The speakers shared with the US-VISIT staff their expert advice on privacy and security

Privacy Complaints & Dispositions:

For the 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. Complaints may be from U.S. Citizens and Lawful Permanent Residents as well as visitors and aliens.[6]

Type of Complaint	Number of Complaints	Disposition of Complaint		
		Responsive Action Taken	No Action Required	Pending
Process and Procedure	1	1	0	2012[7]
Redress	242	62	0	182
Operational	35	2[8]	0	34
Referred	36	36	0	0
Total	314	101	0	2228

The complaints have been separated into four categories for this reporting period. As the reporting is further developed, additional categories may be added.[9]

1. *Process and Procedure.* Issues concerning process and procedure, such as consent, appropriate notice at the time of collection, or notices provided in the *Federal Register*, such as rules and SORNs.
   Example: An individual submits a complaint as part of a rulemaking that alleges the program violates privacy.
2. *Redress*. Issues concerning appropriate access, correction, and redress.
   Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[10]
3. *Operational*. Issues related to general privacy concerns and concerns not related to Transparency or Redress.
4. *Referred.* The DHS Component or the Privacy Office determined that the complaint would be more appropriately handled by another Federal agency or other entity and referred the complaint to the appropriate organization.

---

[6] *DHS Privacy Policy Guidance Memorandum 2007-01*.
[7] This number represents 2012 complaints that were pending from Q4 FY 2008
[8] This number includes a complaint which was pending from Q4 FY2008
[9] During the FY2008 Q4 reporting period, DHS updated its categories to match the categories required for Federal Information Security Management Act (FISMA)/Privacy Reporting described in OMB's Memorandum M-08-21. Based on these changes, "Referred" complaints are now counted separately. In previous reports, "Referred complaints" were categorized as a responsive action.
[10] This category excludes FOIA and Privacy Act requests for access which are reported annually in the Annual FOIA Report

Example: An individual has a question about his or her driver's license or Social Security Number, which we refer to the proper agency.

Dispositions of complaints are reported in one of the three following categories by DHS Components or the Privacy Office:

1. *Responsive Action Taken*. The DHS Component or the Privacy Office reviewed the complaint and a responsive action was taken. For example, an individual may provide additional information to distinguish themselves from someone else.
2. *No Action Required.*[11] The DHS Component or the Privacy Office determined that the complaint does not ask for or require a DHS action or response. Examples are a complaint regarding a published PIA or final rule.
3. *Pending.* The DHS Component or the Privacy Office is reviewing the complaint to determine the appropriate response.

[11] This category has changed since Quarter 2 FY08 reporting. The description of the complaint disposition was changed to better reflect the response to the complaint.

Appendix I

Reviews:
For the purposes of Section 803 Reporting, reviews include the following activities, which may be updated, as appropriate:

1. Privacy Threshold Analyses - DHS's mechanism for reviewing IT systems, programs, and other activities for privacy protection issues, including the appropriate use of Social Security Numbers and information sharing environment (ISE) reviews;
2. Privacy Impact Assessments, required under both the E-Government Act of 2002 and the Homeland Security Act of 2002;
3. System of Records Notices and associated Privacy Act Exemptions;
4. Privacy Act Statements as required under Section (e)(3) of the Privacy Act, which provides notice to individuals at the point of collection;
5. Computer Matching Agreements;
6. Data Mining Activities as defined by Congress under Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007; and
7. Privacy protection reviews of Information Technology and Program Budget requests, including OMB 300s and Enterprise Architecture Alignment Requests through DHS's Enterprise Architecture Board.