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

September 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 4th quarter report for 2008.[5] This report in large part covers the period of June 1, 2008 to September 1, 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. During this reporting period DHS updated it's categories to match the categories required for Federal Information Security Management Act (FISMA)/Privacy Reporting described in Office and Management and Budget (OMB) Memorandum M-08-21.

---

[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 OMB Federal Information Security Management Act (FISMA) IT Security and Privacy reporting.

4th Quarter 2008 Section 803 Report
June 1, 2008 – September 1, 2008

Reviews:

Type of Review	Number of Reviews
Privacy Threshold Analyses	61
Privacy Impact Assessments	22
System of Records Notices and associated Privacy Act Exemptions	11
Privacy Act (e)(3) Statements	1
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Protection Reviews of IT and Program Budget requests	79
Total Reviews for Q4FY08	*174*

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. U.S. Citizenship and Immigration Services (USCIS), a component of DHS, issued a PII Memorandum that explained the policy and procedures of handling PII. USCIS employees were advised on the importance of reporting PII incidents and the ramification for violating the Privacy Act and its principles. The Memorandum was very well received and got maximum results.
2. The U. S. Coast Guard (USCG), a component of DHS, issued Privacy guidance with the following publications: 1) C4&IT Acquisition Microsite Announce Notification, 2) CG Transportation Worker ID Credential (TWIC) Verification & Enforcement Guide, 3) Field Intelligence Support to Operations Manual (FISO), 4) Sensitive Security Information Management Program (SSIMP).

During the reporting period, DHS conducted the following training:

1. DHS personnel and contractors took classroom-based privacy training courses in 3311 instances.

2. DHS personnel and contractors took computer-assisted privacy training courses in 6008 instances.

The Transportation Security Administration released their second poster in their poster campaign related to protecting personally identifiable information.

The U. S. Coast Guard issued CG ALCOAST message entitled "Privacy Incidents and Protection of Personally Identifiable Information (PII)." This directive was disseminated to every member of the CG community (40,000+) and summarized recent privacy incidents and promotes overall awareness and vigilance of PII.

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]

During this reporting period DHS updated it's categories to match the categories required for Federal Information Security Management Act (FISMA)/Privacy Reporting described in Office and Management and Budget (OMB) 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.

Type of Complaint	Number of Complaints	Disposition of Complaint		
		Responsive Action Taken	No Action Required	Pending
Process and Procedure	2020	8	0	2012
Redress	480	331	149	0
Operational	14	13	0	1
Referred	46	46	0	0
Total for Q4 FY08	*2560*	*398*	*149*	*2013*

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

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.

[6] *DHS Privacy Policy Guidance Memorandum 2007-01*.

Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[7]

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.
   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.*[8] 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.

[7] This category excludes FOIA and Privacy Act requests for access which are reported annually in the Annual FOIA Report

[8] This category has changed since Quarter 2 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.