

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

March 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 Act¹, the Privacy Act of 1974², the Freedom of Information Act³, the E-Government Act of 2002⁴, 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 requirements, the Privacy Office is providing its 2nd quarter report for 2008.⁵ This report in large part covers the period of December 1, 2007 to March 1, 2008.⁶ The DHS Office for Civil Rights and Civil Liberties will provide a separate report regarding civil liberties.

DHS may modify complaint categories over time to reflect changes in 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 OMB Federal Information Security Management Act (FISMA) IT Security and Privacy reporting.

⁶ As this is a new reporting structure, certain information covers the time period of October 1 through December 31, 2007. The Department will continue to work to standardize the timeframes for information reporting so that by June 1, 2008 this information is uniform.

2nd Quarter 2008 Section 803 Report

Reviews:

Type of Review	Number of Reviews
Privacy Threshold Analyses	67
Privacy Impact Assessments	14
System of Records Notices and associated Privacy Act Exemptions	3
Privacy Act (e)(3) Statements	2
Computer Matching Agreements	0
Data Mining Reports	1
Privacy Protection Reviews of IT and Program Budget requests	14
<i>Total Reviews for Q2FY08</i>	<i>101</i>

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

Advice & Responses:

During the reporting period, DHS conducted the following training:

1. DHS personnel and contractors took computer-assisted privacy training courses in 2,274 instances.⁷
2. DHS Privacy Office provided ten in-person privacy training courses to DHS personnel and contractors.

⁷ DHS offers multiple computer training courses. An individual may have taken multiple courses if their current job requires such training.

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.⁸

Type of Complaint	Number of Complaints	Disposition of Compliant			
		Responsive Action Taken	Referred	Unable to Assist	Pending
Transparency	46	1	4	0	41
Redress	2,914 ⁹	2,397	510	3	4
General	274	10	263	0	1
<i>Total for Q2 FY08</i>	<i>3234</i>	<i>2408</i>	<i>777</i>	<i>3</i>	<i>46</i>

The complaints have been separated into three categories for this reporting period.¹⁰ As the reporting is further developed, additional categories may be added.

1. *Transparency.* 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.¹¹
3. *General.* Issues related to general privacy concerns and concerns not related to Transparency or Redress.
Example: An individual has a question about his or her driver's license or social security number, which we refer to the proper agency;
Example: An employee's health information was disclosed to a non-supervisor.
Example: A supervisor disclosed personnel file to a future employer.

⁸ DHS Privacy Policy Guidance Memorandum 2007-01.

⁹ This figure includes the number of individuals who filed a redress inquiry with the DHS Traveler Redress Inquiry Program (DHS TRIP) and checked off the box on the online form that reads: "I feel my personal information has been misused." Individuals may check off one or more boxes to capture their concerns. This means that some of the 2,914 noted above may also have identified a civil rights concern, which may result in some duplication of the number of complaints reported by the DHS Privacy Office and the Office for Civil Rights and Civil Liberties.

¹⁰ Based on this new reporting requirement, the complaints for this report cover the time period from October 2007 to February 2008 with different components and DHS headquarters offices reporting different time periods. This will be standardized by the 3rd quarter report.

¹¹ This category excludes FOIA and Privacy Act requests for access which are reported annually in the Annual FOIA Report

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

1. *Responsive Actions 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. *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.
3. *Unable to Assist.* The DHS Component or the Privacy Office determined that the subject of the complaint referred to activities that the Department is authorized to perform.
4. *Pending.* The DHS Component or the Privacy Office is working on 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.