

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

June 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, the Privacy Office is providing its 3rd quarter report for 2008.⁵ This report in large part covers the period of March 1, 2008 to June 1, 2008. The DHS Office for Civil Rights and Civil Liberties will provide a separate report regarding civil liberties.

With this 3rd quarter report, DHS has modified the complaint disposition from “Unable to Assist” to “No action required” to better reflect the nature of the response to such complaints. 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 OMB Federal Information Security Management Act (FISMA) IT Security and Privacy reporting.

3rd Quarter 2008 Section 803 Report

Reviews:

Type of Review	Number of Reviews
Privacy Threshold Analyses	103
Privacy Impact Assessments	13
System of Records Notices and associated Privacy Act Exemptions	7
Privacy Act (e)(3) Statements	1
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Protection Reviews of IT and Program Budget requests	0
<i>Total Reviews for Q2FY08</i>	<i>124</i>

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. Sensitive System Handbook 4300 and 4300A, updated to include additional, privacy-related requirements.
2. Appendix S of 4300A: Compliance Framework NIST SP 800-53 Controls for Privacy Sensitive Systems.
3. Official DHS System of Records Notice (SORN) Guidance, providing guidance on how to write a SORN.
4. Updated Privacy Threshold Analysis.
5. Privacy Act Statement Guidance as related to (e)(3) of the Privacy Act.

During the reporting period, DHS conducted the following training:

1. DHS personnel and contractors took classroom-based privacy training courses in 3795 instances.
2. DHS personnel and contractors took computer-assisted privacy training courses in 59,401 instances.⁶

⁶ DHS offers multiple computer training courses. An individual may have taken multiple courses if their current job requires such training. This number includes annual privacy awareness training for the US Coast Guard and Immigration and Customs Enforcement (ICE).

In addition, the U.S. Coast Guard, a component of DHS, conducted an All Hands Training and Privacy Awareness week for the US Coast Guard members and employees. The Science and Technology Directorate held S&T Privacy Day, which included multiple one hour sessions on protecting privacy. The Transportation Security Administration has begun a poster campaign related to protecting personally identifiable information.

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.⁷

Type of Complaint	Number of Complaints	Disposition of Complaint			
		Responsive Action Taken	Referred	No Action Required	Pending
Transparency	39	3	0	36	0
Redress	630 ⁸	70	17	358 ⁹	185
General	281	114	29	135	3
<i>Total for Q2 FY08</i>	<i>950</i>	<i>187</i>	<i>46</i>	<i>529</i>	<i>4</i>

The complaints have been separated into three categories for this reporting period. 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.

⁷ DHS Privacy Policy Guidance Memorandum 2007-01.

⁸ 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 630 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. The number of redress complaints does not include Privacy Act requests for information or correction. In addition, the number does not include requests for correction as part of credentialing or screening programs at the Department where a redress process has been set up external to the Privacy Act process. For example, Transportation Worker Identification Credential (TWIC) has an appeal process set up to handle correction, misidentification, and other issues related to the TWIC program. Given the similarity between these redress programs and the Privacy Act process, and the fact that OMB M-08-09 specifically states that Privacy Act requests should not be included in the annual Federal Information Security Management Act (FISMA) reporting, DHS has chosen not to include these numbers.

⁹ DHS TRIP Privacy complaints that require additional paperwork or information from the individual are considered "Not Action Required" until the paperwork has been submitted. Upon submission of paperwork, the complaints will be counted as "Pending" or "Responsive Action Taken."

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. *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.

Dispositions of complaints are reported in one of the four 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. *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. *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.
4. *Pending*. The DHS Component or the Privacy Office is reviewing the complaint to determine the appropriate response.

¹⁰ This category excludes FOIA and Privacy Act requests for access which are reported annually in the Annual FOIA Report

¹¹ 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.