



**The Department of the Treasury
Report Pursuant to Section 803 of the
Implementing Recommendations of the 9/11
Commission Act of 2007**

September 30, 2009

Introduction

The Treasury Department is committed to protecting the privacy and civil liberties of individuals, including information privacy, in policy development and program execution. In recognition of the threat to individual privacy by the global expansion of information technology (IT), the Department is continuing robust oversight.

Department Actions

During this reporting period (ending August 31, 2009) the Department reinforced the importance of privacy awareness training Department-wide. As a result, the Department achieved a significant 22% increase in the number of employees who completed the training this year compared to the same period a year ago.

The Treasury Department continues its support of the Federal CIO Council Privacy Committee and co-chairs a workgroup under its Development and Education Subcommittee. This workgroup is planning a Privacy Summit scheduled for this fall. The summit will provide training to privacy professionals across the government, and is designed to provide insight into how privacy officials manage privacy, improving compliance with OMB guidance.

In addition, the new Administration issued its 60-Day Cyberspace Policy Review on May 29, 2009. As part of this effort, the Administration established an Information and Communications Infrastructure Interagency Policy Committee as the primary policy coordination body for issues related to achieving reliable and secure global information and communications infrastructure. Several sub-committees have been formed to further address specific elements, including a subcommittee for Civil Liberties and Privacy Rights. The Department serves on this subcommittee, which is designed to address the privacy and civil liberties communities' concerns with cyberspace technology and policies.

Quarterly Report

The Department uses a standard reporting framework and instructions tailored to its mission and functions to address Section 803 reporting requirements. This framework has been

coordinated with OMB, as well as with the other agencies required to report under this section.

The attached September 2009 report consolidates all privacy and civil liberties activities of the Treasury Department, including data on the reviews conducted, reference to the advisory guidance delivered, and information about written complaints received and processed.

Types of Complaints

Privacy Complaint: A written allegation of harm or violation of personal or information privacy filed with the Treasury Department. This information includes:

1. Process and procedural issues, such as consent, collection, and appropriate notice;
2. Non-Privacy Act of 1974 issues, such as Terrorist Watchlist Redress process or identity theft mitigation; or
3. Privacy Act of 1974 issues.

Civil Liberties Complaint: A written allegation of harm or violation of the constitutional rights afforded individuals filed with the Treasury Department. Types of civil liberties complaints include, but are not limited to:

1. First Amendment, Freedom of speech, religion, assembly, and association;
2. Fourth Amendment, Protection against unreasonable search and seizure; and
3. Fifth or Fourteenth, § 1, Due process and equal protection.

Reporting Categories

Reviews: Reviews include Treasury Department activities delineated by controlling authorities, such as the Privacy Act of 1974, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Circular A-130, Appendix 1; and OMB Memo M-07-16. Examples include:

1. Privacy Threshold Analyses – review of an IT system’s use of data to determine if a Privacy Impact Assessment is required;
2. Privacy Impact Assessments;
3. OMB Memo 07-16 issues, including reviewing records to maintain the minimum necessary for the proper performance of an agency function, Social Security Number use reduction efforts, or initiatives related to combating identity theft;
4. OMB Circular A-130 issues, including System of Records Notices, Routine Use Descriptions, Agency contacts security, Recordkeeping and Disposal policies, Training Practices, Continued Privacy Act Exemptions under 5 U.S.C §552a (j)(2)(k), and/or Computer Matching Programs;
5. Persistent Tracking Technology features used on a website;
6. Achievement of machine readability, which ensures that website users are automatically alerted about whether site privacy practices match their personal privacy preferences;

7. 5 CFR 1320 (collection of information/Paperwork Reduction Act reviews);
8. Information Sharing Environment policies and system reviews;
9. Documents related to the OMB Exhibit 300 process.

Advice: Advice includes written policies, procedures, guidance, or interpretations of privacy requirements for circumstances or business processes that respond to privacy or civil liberties issues or concerns.

Response to Advice: Specific action taken in response to *Advice* given by the Treasury Department. Examples of *Response to Advice* include the issuance of a regulation, order, or directive; an interpretation or other guidance issued as a result of the *Advice*, or the reaching of an agreement; and issuance of any training programs or other procedures that enhance understanding of the issue that precipitated the request for *Advice*.

Dispositions of Complaints: An action taken by the Treasury Department in response to a privacy or civil liberties complaint. After a complaint is reported the Treasury Department will:

1. Take direct action (description in the summary report);
2. Refer to another agency or entity that may be able to assist in addressing the complaint (referral agency and explanation in summary report); or
3. Determine that no action is required (explanation in summary report).

The Department will continue to submit quarterly reports in coordination with OMB. The current report covers data collection from June 1, 2009, through August 31, 2009. The next quarterly report is due December 31, 2009, and will cover the period of September 1, 2009, through November 30, 2009. The data collection period for each report ends approximately 30 days prior to the report deadline.