The Department of the Treasury
FY 2014 Q3 Report on Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007

For the reporting period
March 1, 2014 to May 31, 2014

1. Introduction

The Implementing Recommendations of the 9/11 Commission Act of 2007 ("9/11 Commission Act") requires the Department of the Treasury to appoint a senior officer to serve as its Privacy and Civil Liberties Officer ("Privacy and Civil Liberties Officer" or "PCLO"). Treasury Directive ("TD") 25-09, "Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53," designates the Treasury Assistant Secretary for Management ("ASM") as the Department's PCLO. As the Department's PCLO, the ASM is responsible for implementing the privacy and civil liberties requirements of the 9/11 Commission Act.

To assist the ASM with the aforementioned responsibilities, TD 25-04, "The Privacy Act of 1974, As Amended," designates the Deputy Assistant Secretary for Privacy, Transparency, and Records ("DASPTR") as the ASM's principal advisor on issues related to privacy and civil liberties. The DASPTR leads the Office of Privacy, Transparency, and Records ("OPTR") and provides the ASM with day-to-day support in executing the privacy and civil liberties duties entrusted to his or her capacity as the Department's PCLO.

This report is being published pursuant to Section 803 of the 9/11 Commission Act, which requires the PCLO to periodically, but not less than quarterly, prepare a report on the privacy and civil liberties activities of the Department. Accordingly, below is a summary of the Department's activities for the third quarter of Fiscal Year 2014.

2. Treasury Actions

The Department of the Treasury is committed to protecting the privacy and civil liberties of individuals in all Treasury programs. In recognition of potential threats to individual privacy and civil liberties resulting from global expansion of information technology, the Department continues its vigilant oversight of the personally identifiable information ("PII") entrusted to its care.

Departmental Initiatives
OPTR is working with Treasury bureaus to expand its Privacy Impact Assessment ("PIA") template and manual to include an assessment of both the privacy and civil liberties risks associated with the collection, maintenance, and disposition of PII. The revised template and manual expands coverage beyond the requirements in the E-Government Act of 2002 and Office of Management and Budget ("OMB") Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," to include those responsibilities assigned to the ASM by TD 25-09. When completed and approved, the assessment will be renamed "Privacy and Civil Liberties Impact Assessment" to reflect its broadened scope.

OPTR is leading Treasury's implementation of the new National Institute of Standards and Technology Special Publication 800-53 Appendix J controls. Pursuant to OMB Memorandum 14-04, "Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," the Senior Agency Official for Privacy ("SAOP") is responsible for assessing and implementing the controls. In addition to the role as the Treasury PCLO, the Treasury ASM also serves as the SAOP. As a result, OPTR is working very closely with the Office of the Chief Information Office ("OCIO") to ensure privacy controls are embedded in the appropriate Treasury policies. Revised TD 85-01, "Department of the Treasury Information Technology (IT) Security Program," will assign responsibility for implementing the privacy controls to the DASPTR. The accompanying publication to TD 85-01 will provide guidance for implementing each of the specific controls.

In addition to the aforementioned activities, OPTR continued to conduct other reviews required by the Privacy Act of 1974, as amended, the E-Government Act of 2002, the Consolidated Appropriations Act of 2005, OMB Circular A-130, Appendix 1, "Federal Agency Responsibilities for Maintaining Records About Individuals," and OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." Examples of the reviews conducted under these authorities include Privacy Threshold Assessments ("PTA"), PIAs, investigations and remedial measures to address incidents involving PII, and reviews of documents related to OMB Exhibit 300, "Planning, Budgeting, Acquisition, and Management of Information Technology Capital Assets."

Treasury currently maintains 311 systems containing PII. To increase transparency and provide the public with greater access to information about its systems and their associated safeguards, Treasury posts PIAs and System of Records Notices ("SORN") to the following websites:

PIAs: http://www.treasury.gov/privacy/PIAs
SORNs: http://www.treasury.gov/privacy/issuances

Internal Revenue Service ("IRS") Initiatives
During this reporting period, the IRS continued implementing its comprehensive strategy to prevent identity theft. These efforts focus on eliminating the use of Social Security numbers

(SSN) on payment notices, and protecting tax information by shutting down fraudulent websites and schemes.

The IRS launched the third phase of their SSN elimination project to mask SSNs on payment notices and added Two Dimensional ("2D") Barcodes to four Installment Agreement notices affecting an estimated 33 million notices annually. The 2D Barcode provides IRS with information needed to process the notice and mask the full display of the SSN in the body of the notice by exposing only the last four digits of the SSN. In addition, the IRS enhanced its payment-processing systems to accommodate the 2D Barcode notices processed by these systems. By January 2015, these enhancements will provide SSN masking on 34 individual non-payment notices affecting 17.4 million notices annually.

While attempts to obtain taxpayer information through false IRS websites and other electronic methods continue, the IRS continues to work to identify the sites, and quickly shut these websites down in order to protect taxpayer information and maintain public confidence. Over 200 sites, including 102 schemes related to "Get Your Refund," were shut down this quarter.

3. Quarterly Reporting Matrix

The attached reporting matrix consolidates all Treasury privacy and civil liberties activities during the reporting period, including data on the reviews conducted reference to the advisory guidance delivered, and information about written complaints received and processed.

3.1. Types of Potential Complaints

- *Privacy Complaint*: A privacy complaint is a written allegation filed with the Department concerning a problem with or violation of privacy protections in the administration of the programs and operations of the Department that may be the cause of harm or violation of personal or information privacy. This information may include: Process and procedural issues, such as consent, collection, and appropriate notice;
- Non-Privacy Act of 1974 issues or identity theft mitigation; or
- Privacy Act of 1974 issues.

3.1.2 *Civil Liberties Complaint*: A written allegation filed with the Department alleging harm or violation of an individual's constitutional rights. Types of civil liberties complaints include, but are not limited to:

- First Amendment (Freedom of speech, religion, assembly, and association);
- Fourth Amendment (Protection against unreasonable search and seizure); and

- Fifth Amendment or Fourteenth Amendment, § 1 (Due process and equal protection).

4. Reporting Categories

4.1. *Reviews*: Reviews include Treasury privacy and civil liberties 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 Memorandum 07-16. Examples include:

- PTAs – review of an IT system's use of data to determine whether a PIA is required;
- PIA (soon to be renamed PCLIA) refers to both a risk assessment process and a document representing the output of that process. PIAs are conducted to: identify privacy and civil liberties risks in systems, programs and other activities that maintain PII; ensure that information systems**,** programs and other activities comply with legal, regulatory, and policy requirements; analyze the privacy and civil liberties risks identified; identify remedies, protections and alternative or additional privacy controls necessary to mitigate those risks; and provide notice to the public of privacy and civil liberties protection practices.
- OMB M 07-16 reviews conducted to minimize the volume of PII necessary for the proper performance of an agency function, SSN use reduction efforts, or initiatives related to combating identity theft;
- OMB Circular A-130 reviews consist of reviews of systems of records notices (SORNs), routine use descriptions, agency security contacts, recordkeeping and disposal policies, training practices, continued Privacy Act exemptions under 5 U.S.C §552a (j)(2), (k), and Computer Matching Programs;
- Persistent Tracking Technology features used on a website;
- Achievement of machine readability, which ensures that website users are automatically alerted about whether site privacy practices match their personal privacy preferences;
- Reviews under 5 C.F.R. part 1320 (collection of information/Paperwork Reduction Act);
- Information Sharing Environment Privacy Guidelines Assessment including policies and system reviews; and
- Reviews related to the OMB Circular A-11, Exhibit 300 process.

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

4.3. *Response to Advice*: Specific action taken in response to Treasury advice. Examples of Responses to advice include issuing a regulation, order, or directive; interpreting or otherwise issuing guidance as a result of advice; reaching an agreement related to the advice; and developing training programs or other procedures that enhance understanding of the issue that precipitated the request for advice.

4.4. *Disposition of Complaints*: Treasury action in response to a privacy or civil liberties complaint. In response to a complaint, the Department will:

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

The data collection period for each report ends approximately 30 days prior to the report deadline.