The Department of the Treasury FY 2014 Q2 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 December 1, 2013 to February 28, 2014

1. Introduction

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 (IT), the Department will continue its vigilant oversight of the personally identifiable information (PII) entrusted to its care. In coordination with the Office of Management and Budget (OMB), the Office of Privacy, Transparency, and Records (OPTR) has established a standard reporting framework tailored to the missions and functions of the Department. Accordingly, below is a summary of the functions on which OPTR is required to report pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P. L. 110-53).

2. Treasury Actions

Departmental Initiatives

OPTR is revising 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. Consequently, OPTR is changing the name of the process to a "Privacy and Civil Liberties Impact Assessment (PCLIA)." The revised assessment template and manual will expand the scope of systems and information subject to the assessment requirement.

OPTR conducted other reviews during the reporting period as required by: the Privacy Act of 1974, 5 U.S.C. § 552a; the E-Government Act of 2002 (P.L. 107-347); the Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Circular A-130, Appendix 1; and OMB M-07-16. Examples of the reviews conducted under these authorities include Privacy Threshold Analyses (PTA), PIAs, investigations and remedial measures to address incidents involving PII, and review of documents related to the OMB Exhibit 300 process.

OPTR continues to lead Treasury's implementation of the new National Institues Standards and Technology 800-53 Appendix J controls. Pursuant to OMB Memorandum 14-04, OPTR is conducting an assessment of these controls which will inform its implementation of the

NIST requirements. In addition, OPTR is reviewing and revising its current PIA template. The revised template will include an assessment of both the privacy risks and civil liberties risks associated with the collection, maintenance, and disposition of PII.

OPTR routinely provides guidance to Treasury's bureaus regarding the preparation and completion of PIAs and system of records notices (SORNs). This guidance is intended to strengthen OPTR oversight of the PIA and SORN processes to ensure compliance with Privacy Act and E-Government Act requirements.

Treasury has 311 systems which contain PII. To provide the public with greater access and transparency, Treasury's PIAs and SORNs may be viewed at the following URLs:

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 identity theft strategy. This effort is focused on preventing refund fraud, investigating these crimes, and assisting taxpayers victimized by identity theft. The IRS is also implementing a project that will provide additional safeguards for PII. Work to prevent identity theft and refund fraud continues to grow, with the requirements implementation touching nearly every part of the organization.

Identity Protection Personal Identification Number (IP PIN): The IP PIN is a unique identifier that authenticates a return filer as the legitimate taxpayer at the time the return is filed. The IRS launched a pilot to test the IP PIN in 2011 and issued approximately 250,000 IP PINs for filing season 2012 and 770,000 IP PINS for filing season 2013 to taxpayers who are victims of tax identity theft. In addition, taxpayers from high-risk identity theft areas using an Electronic Filing Personal Identification Number (EFP) now have the option of requesting the IP PIN through IRS eAuthentication services. The IRS is developing a long-term strategy to expand the IP PIN to additional taxpayer populations.

Locking Decedents' Accounts: The IRS developed new processes to stop the growing use of deceased individuals' identity information by criminals to perpetrate tax fraud. The IRS now routinely locks accounts of deceased taxpayers once they no longer have a filing requirement. To date, the IRS locked more than 11 million accounts. Account locking combined with recent legislative changes restricting the Death Master File should prevent criminals from obtaining fraudulent refunds using decedents' personal information.

Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Project: The IRS is implementing the SPIIDE project to advance real-time data protection and reduce e-mail or network based disclosures of PII. SPIIDE screens e-mail for PII and, when found, prevents the e-mail transmission. When the system is fully operational, IRS will have the ability to effectively stop all e-mail or network-based inadvertent disclosures that may occur and prevent data loss. The first release of SPIIDE focuses on preventing the transmission of PII, including social security numbers (SSNs) through unsecured e-mail transmissions to external stakeholders.

3. Quarterly Reporting Matrix

The attached reporting matrix consolidates all Treasury privacy and civil liberties activities, 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 Memo M-07-16. Examples include:

- PTAs – review of an IT system's use of data to determine whether a PIA is required;
- PIA 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 Memorandum 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 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 CFR 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 Department will continue to submit quarterly reports in coordination with OMB. The next quarterly report is due June 30, 2014, and will cover the period of March 1, 2014, through May 30, 2014. The data collection period for each report ends approximately 30 days prior to the report deadline.