The Department of the Treasury Semiannual 2018 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
October 1, 2017 to March 31, 2018

1. Introduction

The Assistant Secretary for Management (ASM) is the Department of the Treasury (Treasury) Privacy and Civil Liberties Officer (PCLO). As the PCLO, the ASM is responsible for implementing the 9/11 Commission Act of 2007's privacy and civil liberties requirements.

To assist the ASM with these responsibilities, Treasury Directive 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 (PTR) and provides the ASM with day-to-day support in executing PCLO duties.

This report is submitted pursuant to section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007,[1] which sets forth the following requirements:

> (f) Periodic Reports –
> (1) In General –
>
> The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—
> (A)
> (i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;
> (ii) to the head of such department, agency, or element; and
> (iii) to the Privacy and Civil Liberties Oversight Board; and

[1] 42 U.S.C. § 2000ee-1(f).

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) Contents –

Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;
(B) the type of advice provided and the response given to such advice;
(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and
(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

The Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126 (July 7, 2014), changed the reporting period from quarterly to semiannually. The semiannual reports cover the following time periods: April – September and October – March. This report covers PCLO activities from October 1, 2017 through March 31, 2018.

2. Privacy Reviews

Treasury reviews programs and information technology (IT) systems that may present privacy risks. Privacy and civil liberties reviews include the following Treasury activities:

a) Privacy and Civil Liberties Threshold Analyses, which are the Treasury mechanism for reviewing IT systems, programs, and other activities for privacy protection issues to determine whether a more comprehensive Privacy and Civil Liberties Impact Assessment is required;
b) Privacy and Civil Liberties Impact Assessments as required by the E-Government Act of 2002;[2]
c) System of Records Notices, as required by the Privacy Act, and any associated Final Rules for Privacy Act exemptions;[3]
d) Privacy Act Statements, as required by the Privacy Act,[4] to provide notice to individuals at the point of collection;
e) Computer Matching Agreements, as required by the Privacy Act;[5]
f) Data Mining Reports, as required by Section 804 of the 9/11 Commission Act of 2007;[6]
g) Privacy Compliance Reviews;
h) Privacy reviews of IT and program budget requests, including Office of Management and Budget Exhibit 300s; and,

[2] 44 U.S.C. § 3501 note.
[3] 5 U.S.C. §§ 552a(j), (k). *See also* Office of Management and Budget (OMB) Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," 81 FR 94424 (Dec. 23, 2016).
[4] 5 U.S.C. § 552a(e)(3).
[5] 5 U.S.C. § 552a(o)-(u).
[6] 42 U.S.C. § 2000ee-3.

i) Other privacy reviews, such as implementation reviews for information sharing agreements.

3. Privacy and Civil Liberties Impact Assessments (PCLIA)

The PCLIA process is one of Treasury's key mechanisms to ensure that programs and technologies sustain, and do not erode, privacy protections. During the reporting period, Treasury published 89 new, updated, or renewed PCLIAs. All published Treasury PCLIAs are available on Treasury's PCLIA website: https://www.treasury.gov/privacy/PIAs/Pages/default.aspx (links are also provided to bureau websites where additional PCLIAs are posted). One example of a new PCLIA is summarized below:

> On November 30, 2017, the Internal Revenue Service (IRS) published a PCLIA for Skype for Business, an internal office collaboration and instant messaging client for internal IRS communications and meetings that is part of the Office Pro Plus 365 suite of tools. Skype is a collaboration tool that enables employees to hold online meetings (video or audio) with IRS co-workers, conduct online peer-to-peer conversations, share information/files, send instant messages, indicate availability (presence) and screen sharing. There is no direct contact with taxpayers as it only provides for communication between IRS users. The tool enables efficient and effective communications, information sharing and rapid collaboration for a wide range of functions including tax administrative, personnel management, performance counseling, and distributed meetings.
>
> IRS Privacy Compliance and Review worked closely with the business unit to address the accuracy and completeness of the Skype PCLIA as well as plain language requirements. Improvements included updating the cited authorities for the collection of personally identifiable information (PII), i.e., personnel administration for manager-employee counseling. PCLIA updates also included clarification of the Skype for Business Usage and Data Privacy Statement.

4. System of Records Notices (SORN)

During the reporting period, Treasury did not publish or update any SORNs. All Treasury SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act exemptions are available on Treasury's SORN website, https://www.treasury.gov/privacy/issuances/Pages/default.aspx. Treasury has determined that the information contained in its systems of records is accurate, timely, relevant, complete, and necessary to maintain the proper performance of a documented agency function. Please consult the SORN website or the Federal Register for the full text of our SORNs.

5. Computer Matching Programs

Treasury participates in 14 active computer matching programs in accordance with the Privacy

Act of 1974, as amended. The computer matching provisions of the Privacy Act improve oversight of the disclosure of automated Privacy Act records in inter-agency information sharing arrangements known as matching programs, and protect the due process rights of individuals whose records are exchanged in such programs. To comply with the Act, as well as all relevant regulations and guidance, Treasury has established a Data Integrity Board to review and approve associated matching agreements. All Treasury Computer Matching Agreements (CMAs) are available on Treasury's CMA website, https://www.treasury.gov/privacy/Computer-Matching-Programs/Pages/default.aspx.

During the reporting period, the Data Integrity Board reviewed and approved one 12-month renewal and two 18-month re-establishment agreements.

a) The Bureau of the Fiscal Service (BFS) and Department of Health and Human Services (HHS) matching program is part of the Do Not Pay Initiative, which seeks to reduce improper federal payments. This matching program allows Treasury/BFS to provide information to HHS that allows the agency to determine an individual or entity's eligibility to participate in federal procurement and or assistance programs or benefits. On August 23, 2017, Treasury approved a 12-month renewal of the matching program, effective October 8, 2017. The original agreement is available at 79 FR 53201.

b) Project 692 – Medicare Prescription Drug Subsidy Program CMA between IRS and Social Security Administration (SSA). This computer matching agreement sets forth the terms, conditions, and safeguards under which the IRS will disclose to the SSA certain return information for the purpose of verifying eligibility for the Prescription Drug Subsidy Program and to determine the correct subsidy percentage of benefits provided under section 1860D-14 of the Social Security Act. (42 U.S.C. § 1395w-114). On September 1, 2017, Treasury approved an 18-month re-establishment of the matching program, effective November 27, 2017. The agreement is available at 82 FR 49691.

c) Project 693 – Income-Related Adjustments to Medicare Premiums CMA between IRS and SSA. This computer matching agreement sets forth the terms under which the IRS will disclose to the SSA certain return information for the purpose of establishing the correct amount of Medicare Part B premium subsidy adjustments and Medicare Part premium increases under section 1839(i) and 1860D-13(a)(7) of the Social Security Act (42 U.S.C. § 1395r(i) and 1395w-113(a)(7)), as enacted by section 811 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA; Pub. L. No. 108-173) and section 3308 of the Affordable Care Act of 2010 (Pub. L. No. 111-148). On December 21, 2017, Treasury approved an 18-month re-establishment of the matching program, effective April 1, 2018. The agreement is available at 83 FR 6666.

6. Privacy Compliance Reviews (PCR)

Treasury conducts PCRs to ensure that programs and technologies implement and maintain appropriate protections for PII. The PCR is a collaborative effort that helps improve a program's

ability to comply with existing privacy requirements by identifying and remediating gaps in compliance documentation, including PCLIAs, SORNs, and formal agreements, such as memoranda of understanding and memoranda of agreement. Treasury conducts informal PCRs with its bureaus when necessary.

During this reporting period, the IRS Privacy Office took a proactive approach to privacy policy development by monitoring emerging issues, identifying gaps, issuing policy, establishing accountability, and providing feedback on related NIST special publications. IRS updated Internal Revenue Manual (IRM), section 10.5.1, Privacy and Information Protection – Privacy Policy, and incorporated Interim Guidance Memos on "Digital Assistants and Other Devices" and "Social Security Number Elimination and Reduction." This cornerstone IRM reorganized to delineate key privacy definitions and concepts, roles and responsibilities, culture (expectations and privacy awareness programs), policy, and other privacy-related programs.

Furthermore, the Controlled Unclassified Information (CUI) program established by Executive Order 13556 standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Because of the volume of data affected by the marking and controls associated with CUI implementation, the IRS will begin implementation with a pilot to identify affected policy, procedures, and terminology before expanding to the rest of the enterprise.

The Office of the Comptroller of the Currency continued to implement its data loss prevention program. Those efforts focused on reducing the risk of disclosure of PII, educating employees about sending PII in a secure manner and preventing the unauthorized removal of PII by removable media and monitoring web activity for PII.

Finally, in October of 2017, Treasury submitted to Congress its report as required by the Social Security Number (SSN) Fraud Prevention Act of 2017. In the report, Treasury stated that the best way to reduce instances where SSNs are included in mailings is to reduce or eliminate the collection of the SSNs for official government purposes whenever feasible. Therefore, Treasury policy only allows the collection, maintenance, and use of SSNs under the following circumstances: (1) security background investigations; (2) interfaces with external entities that require the SSN; (3) a legal/statutory basis (i.e., where collection is expressly required by statute); (4) when there is no reasonable, alternative means for meeting business requirements; (5) statistical and other research purposes; (6) delivery of government benefits, privileges, and services; (7) law enforcement and intelligence purposes; and (8) aging systems with technological limitations combined with funding limitations render impossible system updates or modifications to add privacy risk reduction tools (partial/truncated/redacted or masked SSNs). In the absence of a compelling argument to the contrary, no other SSN uses are allowed. Treasury remains focused on eliminating the use of SSNs whenever possible and safeguarding SSNs that must be collected and maintained because no reasonable alternative exists. Treasury is conducting an analysis of the information obtained in the SSN Fraud Elimination Act data call to determine whether particular SSN collections can either be eliminated or whether additional safeguards can be implemented to limit access to full SSNs, thereby reducing privacy risk. That report is due to Congress on October 15, 2018.

7. Advice and Responses

Treasury provides privacy advice throughout the year to its bureaus and offices. Here is an example of such guidance:

a. The Special Inspector for the Troubled Asset Relief Program (SIGTARP) provided the following advice and guidance related to limiting the use of SSNs in accordance with the SSN Fraud Prevention Act of 2017.
    - Advised the Investigations Division that, when possible, it should use the last four digits of SSNs rather than the entire number. In one instance an agent was unable to use the last four digits and the Office of General Counsel advised that the subpoena be hand delivered. The advice was accepted and acted upon.

8. Privacy Complaints and Dispositions

For purposes of Section 803 reporting, complaints are written allegations of harm or violation of privacy compliance requirements filed with Treasury's privacy and civil liberties programs. The categories of complaints reflected in Appendix A are aligned with the categories detailed in the OMB Memorandum 08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. U.S. citizens, lawful permanent residents, visitors, and aliens may submit complaints.

9. Conclusions

As required by the 9/11 Commission Act, and in accordance with the Intelligence Authorization Act for Fiscal Year 2014, this semiannual report summarizes Treasury's privacy activities from October 1, 2017 through March 31, 2018. Treasury will continue to work with Congress, colleagues in other federal departments and agencies, and the public to continue to protect privacy in all of our activities.

Attachment

Appendix A: Department of the Treasury
Semiannual Report on Privacy and Civil Liberties Activities under Section 803 of the 9/11 Commission Act of 2007
October 1, 2017 through March 31, 2018

Reviews

Type	Number
Privacy Threshold Analyses (PTAs)/Privacy Impact Assessments (PIAs)	PTA/67 PIA/89
System of Records (SOR) Routine Use/ SOR Notices (SORNs)	0
SSN Elimination or Redaction on Forms	2
Computer Matching Agreements (CMAs)	3
Section 508 Internet Website Scan	79%
Treasury-requested Non-Commerce/Commerce Site Scan	Non-Comm/ 3 Comm/ 0

Advice and Response

Type	Number	Response
Provide advice and recommendation regarding handling of PII	4	Accepted
Provide advice and recommendation on policy and procedure	3	Pending/Accepted
Provide advice and recommendation on data collection/ingest review	30	Accepted
Provide advice and recommendation on system requirements/compliance documentation	2	Pending
Provide advice and recommendation on web privacy policies/privacy notices	1	Accepted

Complaints

Type	Number	Dispositions
PRIVACY: Claims taxpayer tax data sent to the wrong taxpayer.	1	Case closed after confirmation there was no disclosure.
PRIVACY: Assertion of unauthorized disclosure	1	Resolved in favor of Government.
CIVIL LIBERTIES: Assertion for violating their 1st, 4th, 5th, 6th, 14th and/or 16th Amendment rights.	5	Pending court date and final decision.
CIVIL LIBERTIES: Assertion for violating their 1st, 4th, 5th and/or 6th Amendment rights.	8	Resolved in favor of Government.
CIVIL LIBERTIES: Plaintiff sought damages and other court costs.	2	Resolved in favor of Government.