The Department of the Treasury Semiannual 2024 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, 2023 to March 31, 2024

1. Introduction

The Assistant Secretary for Management (ASM) is the Department of the Treasury's (Treasury) Chief Privacy and Civil Liberties Officer (CPCLO). As the CPCLO, 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

[1] 42 U.S.C. § 2000ee-1(f).

(iii) to the Privacy and Civil Liberties Oversight Board; and

(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, 2023, through March 31, 2024.

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 (PCLTAs), 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 (PCLIA) is required;
b) PCLIAs as required by the E-Government Act of 2002;[2]
c) System of Records Notices (SORNs), as required by the Privacy Act, and any associated Final Rules for Privacy Act exemptions;[3]
d) Privacy Act Statements (PASs), as required by the Privacy Act,[4] to provide notice to individuals at the point of collection;
e) Computer Matching Agreements (CMAs), 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 (PCRs);
h) Privacy reviews of IT and program budget requests, including Office of Management

[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.

and Budget (OMB) Exhibit 300s; and,

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 165 new, updated, or renewed PCLIAs. The following are examples of PCLIAs for which two bureaus provided summaries:

- The Alcohol and Tobacco Tax and Trade Bureau (TTB) completed 13 Privacy Impact Assessments (PIA(s))/PCLIA(s) during this reporting period for its Tax Major Application (TMA) system and applications, General Support System, and its Regulatory Major Application (RMA) system and applications, as part of continuous monitoring annual testing.

- The Internal Revenue Service (IRS) completed 148 PIA(s)/PCLIA(s) during the reporting period. Among them are: PCLIA for Direct File System. Direct File is a cloud-based application that enables qualified taxpayers to authenticate themselves and respond to an interview-style set of questions to complete their tax returns. The IRS also completed a PCLIA for eGain Solve – Secure Message. The eGain Solve™ software suite provides the opportunity to exchange communique and information between IRS Assistors and taxpayers/authorized representatives using Secure Messaging, Chat, and/or Virtual Assistant (aka Chatbot). Secure messaging creates secure message centers for taxpayers, their representatives, and other third parties. Once authenticated, a taxpayer can log into their inboxes in the Secure Message Center to view or respond to messages with IRS employees, who can then reply on the same secure channel. This helps ensure that sensitive information shared during this exchange between the IRS employee and taxpayer are not exposed to external networks and are thus put at less risk. Secure messages do not interact with mail servers and are used to communicate sensitive and/or important information in a secure environment. For IRS employees, secure messages are handled by workflows, which direct incoming messages to the appropriate IRS employee who logs in to the secure message center to manage messages. For taxpayers and their authorized representatives, secure messages can only be accessed after they have signed into their Secure Messaging portal, which is only accessible by authenticated customers. When a taxpayer is sent a new secure message, they receive a notification informing them that there is a message for them in the Secure Messaging Center. To read the message, they must log in to

their secure message center. Secure messages cannot leave the application and cannot be viewed by customers unless they have authenticated.

All published Treasury PCLIAs are available on Treasury's Privacy website: https://home.treasury.gov/footer/privacy-act/privacy-and-civil-liberties-impact-assessments.

4. System of Records Notices (SORN)

During the reporting period, Treasury did not publish any new SORNs but updated 6 existing SORNs. 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. All Treasury SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act exemptions are available on Treasury's SORN website, https://home.treasury.gov/footer/privacy-act/system-of-records-notices-sorns.

5. Computer Matching Programs (CMAs)

Treasury participates in 3 renewed 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. These provisions also 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 established a Data Integrity Board to review and approve matching agreements. All Treasury CMAs are available on Treasury's CMA website, https://home.treasury.gov/footer/privacy-act/computer-matching-programs.

6. Privacy Compliance Reviews (PCRs)

Treasury conducts PCRs to ensure that programs and technologies implement and maintain appropriate protections for personally identifiable information. 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 and offices when necessary. Informal PCRs are also sometimes done as part of other requirements, such as the Treasury PCLIA requirement and reviews of particular issues required in external reports to Congress.

7. Advice and Responses

Treasury provides privacy and civil liberties advice to its bureaus and offices throughout the year. Some of this advice originates from *ad hoc* responses PTR provides to bureaus and offices, as requested. Other advice originates from discussions within Treasury bureaus, between the bureaus' privacy and civil liberties stakeholders (including legal counsel, as necessary) and systems owners, program managers and staff. PTR and the bureau privacy and civil liberties stakeholders also provide advice during the PCLIA process, advising system owners and program managers on Privacy Act, records management, Paperwork Reduction Act, and other

requirements to ensure they fully comply with applicable laws in the operation of their information systems.

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 are reflected in Appendix A below.

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, 2023, through March 31, 2024. 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.

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, 2023 through March 31, 2024

Reviews	
Type	**Number**
Privacy (and Civil Liberties) Threshold Analysis (PTAs/PCLTAs)	39
Privacy (and Civil Liberties) Impact Assessments (PIAs/PCLIAs)	165
System of Records (SOR) Routine Use/ SOR Notices (SORNs)	6
Computer Matching Agreements (CMAs)	3

Advice and Response		
Type	**Number**	**Response**
Provide advice and recommendation regarding proper handling of PII/limiting access based on need to know	8	1- Bureau of Engraving and Printing (BEP), 4- Treasury Office of Inspector General (TOIG), & 3 – Internal Revenue Service (IRS) Accepted
Provide advice and/or recommendation on relevance and necessity of data collection/ingestion	1	1-TOIG Accepted
Provided guidance to system owners or personnel on necessary privacy compliance documentation or appropriate NIST risk rating.	8	2 -BEP, 1 -TIGTA, 1 U.S. MINT, & 3- TOIG Accepted 1 -U.S. Mint Pending/In Process
Provide advice and recommendation on internal/external sharing of PII (including Privacy Act info)	7	1-U.S. Mint, 1-TIGTA, 3 -IRS, 1-BEP, & 1-TOIG Accepted
Provide advice and recommendation on web privacy policies/privacy notices	1	1-IRS Accepted

Complaints		
Type of claim or assertion in complaint	**Number of complaints**	**Disposition**
PRIVACY: Unauthorized disclosure (internal/ external)	Internal: 0 External: 11	3-IRS External Pending final decision. 8 – TOIG Closed (General information not an OIG matter).
PRIVACY: Collection	6	5-TOIG Closed (General information not an OIG matter). 1-IRS Closed
PRIVACY: (Other: Describe)	1	1-IRS Closed and referred to appropriate department/bureau
CIVIL LIBERTIES: Violation 1st, 4th, 5th, 6th, 14th and/or 16th Amendment rights	4	4- TOIG Closed (General information- not an OIG matter) *or* no TIG nexus
CIVIL LIBERTIES: (Other: Describe)		