Department of the Treasury

2017 Annual Privacy, Data Mining, and Section 803 Reports

Message from the Assistant Secretary for Management

On behalf of the Department of the Treasury, I am pleased to present Treasury's Annual Privacy Report and the Annual Data Mining Report, as required by Section 522 of the Consolidated Appropriations Act of 2005 and the Federal Agency Data Mining Reporting Act of 2007, respectively. This year, for the first time, Treasury is also including in this report the second semi-annual privacy and civil liberties report required under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. Treasury is combining these three separate reporting requirements into a single report and will continue to do so going forward.

Inquiries about these reports may be directed to privacy@treasury.gov. These reports, as well as previous reports, can be found on the Department's Privacy Act website.

J. Trevor Norris

Acting Assistant Secretary for Management
U.S. Department of the Treasury

2017 Annual Privacy, Data Mining, and 803 Reports

Table of Contents

Statutory Requirements

In this report, Treasury consolidates the following three reporting requirements to reduce duplication and to provide Congress and the public with a more comprehensive overview of Treasury's privacy compliance and oversight activities:

(1) The Annual Privacy Report required by Section 522(a) of the Consolidated Appropriations Act of 2005;

(2) The Data Mining Reporting Act requirement contained in Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee–3; and,

(3) The second semi-annual privacy and civil liberties report required under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

The Reporting Periods

These reports cover Treasury activities during the 2017 fiscal year (FY2017) (the reporting period). The two annual reports cover the entire reporting period while the Section 803 report covers the second half of FY2017. The first Section 803 report for FY2017 is a standalone report and can be found on Treasury's Privacy Act website at: https://www.treasury.gov/privacy/annual-reports/Pages/default.aspx.

The Consolidated Appropriations Act of 2005, Annual Privacy Report

The Annual Privacy Report was prepared in accordance with Section 522(a) of the Consolidated Appropriations Act of 2005, which includes the following requirement:

Privacy Officer—

Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including—

* * *

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 552a of title 5, 11 United States Code, internal controls, and other relevant matters;

* * *

The Data Mining Reporting Act of 2007, Annual Report

The Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3, includes

the following requirement:

(c) Reports on data mining activities by Federal agencies

(1) Requirement for report - The head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency under the jurisdiction of that official. The report shall be produced in coordination with the privacy officer of that department or agency, if applicable, and shall be made available to the public, except for an annex described in subparagraph (C).

(2) Content of report - Each report submitted under subparagraph (A) shall include, for each activity to use or develop data mining, the following information:
- (A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.
- (B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.
- (C) A thorough description of the data sources that are being or will be used.
- (D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.
- (E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.
- (F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.
- (G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to—
  - (i) protect the privacy and due process rights of individuals, such as redress procedures; and
  - (ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

The Implementing Recommendations of the 9/11 Commission Act of 2007, Privacy and Civil Liberties Report

Section 803 of the 9/11 Commission Act, 42 U.S.C. § 2000ee-1, 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.

(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.

SECTION ONE: DEPARTMENT OF THE TREASURY FY2017 CONSOLIDATED APPROPRIATIONS ACT OF 2005 ANNUAL PRIVACY REPORT

Oversight and Compliance

For Treasury to accomplish its mission, it must collect personally identifiable information (PII) from its employees and the public, as well as from various organizations and other government agencies. The Department is responsible for managing and protecting the information it collects, maintains, and discloses. Federal law, regulations, and policies govern these activities and are designed to maintain the public's trust.

System of Records Notices (SORN)

A system of records is a grouping of paper or electronic records maintained by a federal agency from which information about an individual is retrieved by the name of the individual or another unique identifier assigned to the individual (e.g., Social Security number). Pursuant to 5 U.S.C. § 552a(e)(4), agencies are required to publish a SORN in the Federal Register for each system of records. Treasury has published regulations describing how it collects, maintains, and discloses records about individuals that are maintained in a system of records. These regulations provide procedures by which individuals may request access to their information maintained by Treasury.[1]

During FY 2017, the Department published one new SORN in the Federal Register: Department of the Treasury, Bureau of Engraving and Printing (BEP) .051 – Chief Counsel Files System of Records, November 4, 2016 (81 FR 77003).

During FY 2017, the Department published 58 reissued and renewed SORNs in the Federal Register:

- Department of the Treasury, BEP .046 – Mutilated Currency Requests Tracking System, August 9, 2017 (82 FR 37290).
- Treasury republished its Treasury-wide systems of records inventory, including 16 SORNs, in the Federal Register on November 7, 2016 (81 FR 78266).
- Departmental Offices republished its systems of records inventory, including 41 SORNs, in the Federal Register on November 7, 2016 (81 FR 78298).

Treasury maintains approximately 177 systems of records, nearly 49 percent of which are maintained by the Internal Revenue Service (IRS). The entire Treasury SORN collection was updated in 2017 as part of the biennial review process required by the Privacy Act of 1974. A complete list of the Department's SORNs is available on Treasury's Privacy Act website at: https://www.treasury.gov/privacy/annual-reports/Pages/default.aspx.

[1] *See* 31 C.F.R. §§ 1.20-1.36.

Privacy and Civil Liberties Impact Assessments (PCLIA)

A Privacy and Civil Liberties Impact Assessment (PCLIA) is an analysis of how information is handled in compliance with legal, regulatory, and policy privacy requirements. It allows the assessment of the risks and effects of collecting, maintaining, and disseminating information and discusses the mitigation strategies used to address those risks. Section 208 of the E-Government Act of 2002 (E-Gov Act) requires agencies to conduct PCLIAs for electronic information systems and collections that involve the collection, maintenance, or dissemination of information in identifiable form from or about members of the public.

In FY 2017, Treasury reviewed 169 PCLIAs. Treasury currently has 245 information technology systems that require a PIA. Pursuant to the E-Gov Act, agencies are required to make PCLIAs publicly available through the agency website, the Federal Register, or other means. The Department's PCLIAs are available on Treasury's Privacy Act website at: https://www.treasury.gov/privacy/annual-reports/Pages/default.aspx.

Federal Information Security Management Act of 2002

The Federal Information Security Management Act of 2002 (FISMA) requires each agency to develop, document, and implement an agency-wide program to provide security for the information and information systems that support its operations. In addition, FISMA requires Chief Information Officers, Inspectors General, and the Senior Agency Officials for Privacy (SAOP) to respond annually to information security questions from the Office of Management and Budget (OMB). OMB also requires SAOPs to report on performance metrics related to the management of their privacy programs. This entails tracking and reporting the number of Treasury systems that contain PII, and the number of systems that require and/or have completed a PCLIA and/or SORN.

For FY 2017, the Department reported a total inventory of 249 FISMA systems that are used to create, collect, use, process, store, maintain, disseminate, and/or disclose PII.

Treasury's Compliance with Privacy-Related Requirements in OMB M-16-04

In FY 2017, Treasury continues to identify its High Value Assets (HVAs) to comply with the OMB Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (OMB M-16-04). OMB M-16-04 defines HVAs as

> assets, systems, facilities, data and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.

Treasury identified as HVAs 49 Treasury systems containing PII. The IRS HVA systems are part of its Privacy Continuous Monitoring process which includes PCLIA updates based on Information Technology (IT) Change Management, annual reviews of SORNs, reporting on

privacy training compliance by system staff, and reviews of audit records for unauthorized access and disclosures. All HVA systems that require PCLIAs or updated PCLIAs either had them or were in the review process. Updated SORNs for all HVA systems were current and up-to-date.

Treasury's Compliance with Privacy-Related Requirements in OMB M-17-06

In FY 2017, Treasury updated its websites to comply with OMB Memorandum 17-06, *Policies for Federal Agency Public Websites and Digital Services* (OMB M-17-06). Specifically, the IRS continues to enhance its FY 2016 effort on the implementation of a privacy page improvement plan to comply with OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, and OMB M-17-06 requirements. The IRS uploaded matching notices, SORNs, and publicly available privacy policies in a timely manner and updated any new exemptions to the Privacy Act requirements and Privacy Act implementation rules to reflect the new exemptions. The IRS achieved full compliance with OMB M-17-06 in early June. Additionally, BEP established a internet domain (https://www.moneyfactorystore.gov/), which is linked to Treasury's Privacy Policy site.

Elimination of the Unnecessary Use of Social Security Numbers

Treasury-wide Assessment of SSNs Sent through the Mail as Required by the Social Security Number Fraud Prevention Act of 2017

In the last quarter of FY2017, Congress required government agencies to report on the title and identification number of any document used during the previous year that included the complete Social Security account number (SSN) of an individual. The law also required government agencies to provide a plan that describes how they will eliminate SSNs from any document sent by mail unless the head of the agency determines that the full SSN is necessary.

During the last quarter of FY2017, Treasury conducted a data call to identify the documents that met the requirements of the SSN Fraud Prevention Act and began the draft of the report which was due in the first quarter of FY 2018. Further information on Treasury's compliance with these requirements will be discussed in Treasury's FY2018 Consolidated Appropriations Act of 2005 Annual Privacy Report.

Internal Revenue Service (IRS)

In FY2017, the IRS continued its efforts to develop and implement written policy and is developing updated guidance and an Internal Revenue Manual section related to the collection or use of SSNs. The IRS continues to address the use of SSNs and reduce the use of unnecessary SSNs through its SSN Elimination and Reduction program.

This program made significant strides in eliminating or reducing the use of SSNs within systems, forms, notices, and letters where the collection or use of the SSN was not necessary. The IRS is systematically reviewing all existing and new notices, letters, and forms for unnecessary SSN use. As of FY 2017, the IRS eliminated or reduced the use of the SSNs on 138

payment and non-payment notices, with an estimated annual volume of 50 million taxpayer mailings. The IRS also identified a total of 1,745 letters and 749 IRS forms containing SSNs and has committed to remove or mask SSNs or obsolete the document altogether for 44% (764) of the letters and 28% (206) of the forms. Those letters and forms retaining SSNs must have a statutory/regulatory requirement or a confirmed business need to do so. Wherever possible, the IRS is using a Truncated Taxpayer Identification Number (TTIN). A TTIN can sometimes be used as an alternative to using an SSN, IRS Individual Taxpayer Identification Number (ITIN), or IRS Adoption Taxpayer Identification Number (ATIN). The filer of certain information returns may use a TTIN on the corresponding payee statements to identify the individual being furnished a statement. To further protect identities, the TTIN displays only the last four digits of an individual's identifying number and is shown in the format XXX-XX-1234 or ***-**-1234.

The IRS recently submitted proposed regulations 26 CFR Parts 1, 31, and 301, Use of TTINs on Forms (Wages and Tax Statement) W-2, furnished to employees. This document contains proposed amendments to the regulations under Internal Revenue Code (26 U.S.C.) sections 6051 and 6052, and affects employers who are required to furnish Forms W-2, and employees who receive Forms W-2. To aid employers' efforts to protect employees from identity theft, these proposed regulations would amend existing regulations to permit employers to voluntarily truncate employees' SSNs on copies of Forms W-2, that are furnished to employees. These proposed regulations would also amend the regulations under section 6109 to clarify the application of the truncation rules to Forms W-2.

Bureau of the Fiscal Service

The Bureau of the Fiscal Service (FS) maintains SSNs in its IT systems and programs. Those programs are maintained by various sub-organizations. Detailed descriptions of the activities that are engaged in the reduction or elimination SSNs in IT systems and programs are listed below:

FS Retail Security Services is working to mask the SSN used on the forms and/or documents generated out of its systems and programs.

The following information refers to SSNs held in FS's Fiscal Accounting (FA) systems and programs:

- FS's FA special purpose securities program maintains PII (including SSN), which is stored in InvestOne's accounting software in support of the Federal Housing Administration (FHA) Debenture Program. However, the PII is not unmasked in any of the program's external reports that are shared or posted to any website. The Special Investments Branch has two reports that contain PII: Taxpayer Identification Number (TIN) and a Statement of Accountant (SOA) reports. The PII is unmasked in the TIN Report, but it is only used for internal purposes. The SOA is available both internally (with PII unmasked), and can be requested by FS's customers on an as needed basis (with the PII masked).
- The Funds Management program does not request or maintain SSNs as part of its daily functions. However, the check processing function occasionally receives checks from members of the public that contain SSNs. When these checks cannot be deposited due to

insufficient information to process the deposit, our practice is to return the check to the original sender, unedited. FS does not alter the check, and returns it to the original sender in its original condition.

The following information refers to SSNs held in FS's Payment Management (PM) systems and programs:

- FS's PM systems and programs include the Philadelphia Financial Center (PFC), which provides exception processing services to over 300 federal agencies. PFC has a current business agreement with the Social Security Administration (SSA) that requires PFC to process post payment actions with the SSN printed and/or displayed on respective forms so that SSA is able to process these actions effectively and efficiently. However, over the last few years, FS has conducted reviews of post payment forms/documents that are mailed to financial institutions and to payees and started to systematically truncate SSNs on some of the forms such as the Automated Clearing House (ACH) notifications of reclamation. PFC plans to target other forms such as the check claim, ACH notification of account change, and the ACH trace request form to look for opportunities to truncate/eliminate SSNs without impeding operations.
- PM's Resource Management Division (RMD) may receive privacy release form and background information relating to constituent cases being resolved in response to Congressional inquiries. In some cases, the information must be forwarded to the responsible Federal Agency for resolution actions. In those cases, the SSN may be included as part of a privacy release form that is forwarded with the case background information. RMD is discussing alternative protocols to eliminate transfer of the SSN to the federal agency via email.
- PM's Electronic Funds Transfer (EFT) Strategy Division forwards Direct Express EFT/payment questions to Federal Reserve Bank of Dallas/Comerica for resolution/action. Such transmissions may contain SSNs. EFT Strategy Division will stop using SSNs in this process.

The following information refers to SSNs held in FS's Revenue Collections Management systems and programs:

- The Over the Counter Network (OTCnet) Application does not require the use of SSNs, however, there are currently 27 forms (approximately 10% of all forms) where agencies request the full SSN. OTCNet is working to identify a unique identifier to replace SSN on old forms. These forms will be modified and/or updated to eliminate SSNs once agencies have identified a replacement for SSN identifiers. The OTCnet team plans to modify/update forms to eliminate SSNs in a release scheduled for August 2018. OTCnet also plans to implement Oracle Transparent Data Encryption (TDE) in mid-2018 to further protect sensitive data, including SSNs stored in the OTCnet database. An analysis will be conducted with agencies to determine if historical data in the OTCnet archive and transactional databases can be masked or eliminated.
- IRS Lockbox is a program through which Treasury agrees to let certain financial institutions process individual and business tax payments to help the IRS collect taxes. IRS Lockbox does not send SSNs to electronic check processing or any other FS system.

However, the IRS Lockbox network of financial institutions does send SSNs electronically to the IRS directly through dedicated lines (Axway) in which the SSNs are encrypted. The IRS Lockbox utilizes two-dimensional barcode technology which is a graphical image that contains taxpayer information, including the SSN. These barcodes are scanned into the system, limiting manual entry and access to sensitive taxpayer data.

- Due to agency system limitations, Electronic Federal Tax Payment System (EFTPS) cannot eliminate the use of SSNs. EFTPS has a mainframe encryption project under the cybersecurity mandate for implementation at the end of 2nd Quarter 2018, which will protect the SSN/PII. The first 5 digits of SSNs are masked in all EFTPS taxpayer correspondence (only the last 4 digits are visible).

The following information refers to SSNs held in FS's Debt Management Services systems and programs:

- TINs are masked in all Treasury Offset Program (program through which delinquent debts owed to federal agencies and states are collected), and Cross Servicing (CS) (program that collects delinquent, non-tax debt on behalf of federal agencies) production letters. The program's letter overlays (templates) were modified to present only the last 4 digits of the TIN or to eliminate TINs completely. Going forward, whatever is printed is what will be visible in the Integrated Document Management System (IDMS). FS captures the complete TIN in index fields that are transmitted to both SSA and IDMS, but they are not routinely visible to users in the documents themselves. The TIN is a key field and is displayed in a list associated with each document when an IDMS user initiates a query. That reference in IDMS could be removed from the screen, but it could not be removed from the system because there is no other way to ensure all documents to a particular debtor can be displayed together.

Financial Crimes Enforcement Network (FinCEN)

In FY 2017, FinCEN reviewed its SSN uses and practices, especially those involving transmission of SSNs from FinCEN to outside entities. FinCEN has statutory obligations under the Bank Secrecy Act (BSA) and the USA PATRIOT Act to deter and detect criminal activity and safeguard financial systems from abuse. This is achieved in large part by the collection, maintenance, and sharing of financial information with law enforcement and regulatory agencies. This information typically includes SSNs for the individuals who are the subjects of reporting mandated by FinCEN regulations. Given the unique role that SSNs currently play in identifying individuals in the United States, it is not currently practicable for FinCEN to eliminate the collection or use of SSNs. The transmissions are done by password-protected email or by authenticated, system-to-system, encrypted portal transmissions. FinCEN processes for FOIA/Privacy Act responses are sent in postal mail and may include the full SSN on papers inside the envelope. Response items which include Security Clearance and/or other OPM-related responses require a full SSN per OPM. FinCEN verified that its business processes do not include any need or approved process for postal mail of any of its eleven forms that contain SSNs. However, there are circumstances where a FinCEN form may be emailed or sent by courier.

Privacy Awareness and Training

A Culture of Privacy Awareness

In M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB required agencies to train employees on their privacy and security responsibilities before granting them access to agency information and information systems. Additionally, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Ninety-seven percent of all Treasury employees completed annual privacy awareness training during the reporting period.

IRS Privacy Training

Annual Privacy and Unauthorized Access to Taxpayer Accounts (UNAX) training is mandatory for all IRS employees. Treasury continuously updates these training modules to address emerging issues, support new directives, and meet business needs. For example, the UNAX training includes three video vignettes depicting current, real-life workplace dilemmas and the resulting violations applicable when policies are not followed.

In FY 2017, the IRS monitored the use of the privacy training series implemented in FY 2016. The courses are virtual, interactive and available on demand through the IRS Enterprise Learning Management System. The series includes:

1. IRS Privacy Foundation Training;
2. Privacy Training for IT Specialists;
3. Privacy Training for IT Designers;
4. Enterprise Architecture and Data Strategy Officers Privacy Training; and
5. Cybersecurity Privacy Training

The IRS Privacy Foundation Training is supplemented by four role-based, tactical privacy courses for technical employees including Project Managers, Privacy & Civil Liberties Impact Assessment Preparers, Business Subject Matter Experts, and Adaptive Privacy Impact Assessments Preparers.

Appropriate, on-demand privacy training is equally important for IRS contractors. Therefore, IRS overhauled its Privacy Act training to highlight emerging privacy policy issues and make the training more applicable to a wider audience including contractors. Additionally, 299 Contracting Officer Representatives were trained in FY 2017 on how to ensure proper privacy, security, and disclosure clauses are included in contracts and enforced. Because these clauses are a critical step in protecting privacy during contract execution and closeout, the IRS simultaneously conducted contract review training for key privacy staff members.

Bureau of the Fiscal Service (FS) Privacy Training

In FY 2017, the Bureau of the Fiscal Service reported 100% completion of privacy awareness training that is required for all employees. The FS privacy policy states that each "employee shall receive privacy awareness training annually. Individuals in specific privacy roles

may be required to take specialized training in addition to the annual privacy awareness training required for all employees." The FS relies on business program managers to determine which employees require additional privacy training based on their duties and access to sensitive PII. The program managers determined that the annual privacy awareness training provides a curriculum adequate to the needs of most employees who handle PII as part of their normal work duties. However, FS has determined that a minimum of eight hours of annual specialized/role-based privacy training is required beyond the annual awareness training for personnel in roles directly associated with the Privacy Program and governance process. Those roles include the Chief Privacy Officer, Privacy Act Officer, Senior Privacy Analyst, and Privacy Analyst assigned to support the FS Privacy Program.

Bureau of Engraving and Printing (BEP) Privacy Training

In FY 2017, Treasury's Bureau of the Engraving and Printing reported 90.3% completion of privacy awareness training that is required for all employees. BEP also developed a tailored privacy training module that focuses on the Privacy Act, Incident Handling, and Safeguarding PII. BEP's privacy office presented this training to the BEP Office of Human Resources. The module will be tailored for and presented to other BEP offices/stakeholders throughout FY 2018.

Advancements in Privacy Policy and Protection

The Privacy Act of 1974 and Amendments require each agency to promulgate rules for compliance with the Act. Treasury's bureaus have been proactive with compliance by continually monitoring changes in their processes and developing appropriate privacy policies and protections. Their proactive approach to policy and protection advancements allows the bureaus to stay ahead of evolving technologies and policies to remain in compliance with the Act.

IRS Advancements in Privacy Policy and Protection

The IRS takes a proactive approach to privacy policy development by monitoring emerging issues, identifying gaps, issuing policy, and establishing accountability. In 2017, the IRS issued Interim Guidance on "Digital Assistants and Other Devices," which provides specific policy regarding methods for protecting privacy when working around digital assistants and other devices that can record and/or transmit sensitive audio or visual information in the work/telework environment. These devices and applications include the following examples:

- Digital assistants (such as Dot or Echo hardware using Alexa software, HomePod using Siri)
- Voice-activated devices and smartphone applications (such as Siri, Google Now ("Okay Google"), or Alexa on phones, tablets)
- Internet-connected toys (Cloud Pet, Smart Toy, Hello Barbie, etc.) that might record and transmit
- Security systems and webcams in the telework environment
- Smart TVs or auxiliary equipment (if they include voice activation)
- Operating systems/applications (such as Windows 10, Cortana) that allow voice

commands

- Home surveillance, security, and video/audio: webcams on personal devices in the home, security cameras/microphones

Bureau of the Fiscal Service (FS) Advancements in Privacy Policy

The Bureau of the Fiscal Service privacy policy was first published in December 2016 to establish FS requirements for the recommended processes and procedures for determining whether, and how, FS will collect, maintain, use, or share PII. The privacy policy describes the requirements governing FS PII. Prior to initiating a new collection or use of PII, FS program areas must conduct a risk analysis that documents what PII will be collected, from where, who will have access, what security controls should be put into place, and whether legal authority exists for the collection and anticipated use of PII. In consultation with FS's chief privacy officer and chief counsel, FS programs determine whether and how the Privacy Act applies. Consideration is given to whether personal data will be retrieved by name or personal identifier and whether the system can be operated without personal identifiers as a statistical system. The FS PTA template may be used to conduct and document the PII risk analysis if no other tools are available or suitable for this purpose.

In 2017, FS updated the PTA template, usually seen as a document used to determine if a full PCLIA is required. FS expanded the purpose of the PTA, and it is now used to gather more privacy related risk data about the system and allows the FS CPO to make more informed determinations about the systems during initial and subsequent PTA reviews. FS now requires that all systems update their PTA annually as a privacy risk management and analysis tool.

Leadership and Coordination within Treasury

Executive Order (E.O.) 13636: Improving Critical Infrastructure Cybersecurity

In 2013, the President signed E.O. 13636, *Improving Critical Infrastructure Cybersecurity*, stating: "[i]t is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

To ensure the inclusion of privacy and civil liberties protections in activities under the Order, section 5(a) of the E.O. required federal agencies to coordinate E.O. 13636-related cybersecurity activities with their SAOP. Section 5(b) further required the SAOP to conduct an assessment of their agency's activities under the Order. As required, OPTR conducted a privacy and civil liberties assessment of the Department's cybersecurity activities under the E.O. and submitted its assessment to the Department of Homeland Security (DHS) for inclusion in a consolidated public report. The consolidated report is available on the DHS website at: https://www.dhs.gov/publication/executive-order-13636-privacy-civil-liberties-assessment-report-2016.

Treasury Computer Matching Programs

Pursuant to the Computer Matching and Privacy Protection Act of 1988,[2] Treasury maintains a Data Integrity Board (DIB) to oversee its computer matching programs. Computer matching programs provide a direct benefit to the public by, for example, assisting in the elimination of errors and in monitoring waste, fraud, and abuse.

In FY 2017, the Treasury DIB reviewed and approved six renewals of computer matching programs and re-established three of the Department's ongoing computer matching programs. Matching agreements expire in 18 months after execution unless renewed for an additional 12-month period. After a renewal expires, an agreement may be re-established for an additional 18 months.

Published notices for Treasury's ongoing computer matching programs are available on Treasury's Privacy Act website at: https://www.treasury.gov/privacy/annual-reports/Pages/default.aspx.

[2] Pub. L. No. 100-503.

Table 1 - FY2017 DIB Actions

Agencies Involved	CMA Title	Action	Date of Action
Bureau of the Fiscal Service (FS) - Social Security Administration (SSA)	CMA 1304 – Medicare Part D Prescription Benefit Program	Renewal	September 11, 2017
FS - Department of Health and Human Services (HHS)	CMA 1402 – Do Not Pay Initiative	Renewal	August 22, 2017
FS – Department of Housing and Urban Development (HUD)	Disclosure of identifying information to detect suspected instances of programmatic fraud, waste, and abuse (FW&A)	Establishment	November 10, 2016
Internal Revenue Service (IRS) – Department of Justice (DOJ)	Taxpayer Address Request Program	Re-establishment	April 26, 2017
IRS – SSA	Disclosure of Information to Federal, State, and Local Agencies	Renewal	June 21, 2017
IRS – SSA	Prescription Drug Subsidy Program IRS Project 692	Re-establishment	September 1, 2017
IRS – SSA	Income-Related Adjustment to Medicare Premiums IRS Project 693	Renewal	March 9, 2017
IRS – HHS	Center for Medicare & Medicaid Services Insurance Affordability Programs and Exemptions	Renewal	August 8, 2017
IRS - Treasury Inspector General for Tax Administration Match	Detection and Deterrence of FW&A in IRS Programs, and Operations	Renewal	January 12, 2017

SECTION TWO: DEPARTMENT OF THE TREASURY FY2017 DATA MINING REPORTING ACT OF 2007 ANNUAL REPORT

The Role of the Treasury Chief Privacy and Civil Liberties Officer (CPCLO)

The Department of the Treasury (Treasury or the Department) is providing this report to Congress pursuant to Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Commission Act), entitled the *Federal Agency Data Mining Reporting Act of 2007* (Data Mining Reporting Act or the Act). This report discusses activities currently deployed or under development in the Department that meet the Data Mining Reporting Act's definition of data mining. The report also provides the information the Act requires with respect to each data mining activity.

Definitions

(1) DATA MINING. The term "data mining" means a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where:

a. a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

b. the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

c. the purpose of the queries, searches, or other analyses is not solely—

i. the detection of fraud, waste, or abuse in a Government agency or program; or

ii. the security of a Government computer system.

(2) DATABASE. The term "database" does not include telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources.[3]

Three Treasury bureaus maintain systems using applications that meet the definition of data mining: the Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Service (IRS), and the Alcohol and Tobacco Tax and Trade Bureau (TTB). These systems were discussed in previous Treasury data mining reports.

[3] 42 U.S.C § 2000ee-3(b)(1). "[T]elephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources" are not "databases" under the Act. § 2000ee-3(b)(2).

Treasury Data Mining Activities

IRS Data Mining Activities

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

Four divisions of the IRS are engaged in data mining activities covered by the Act: IRS Criminal Investigation (IRS-CI); the IRS Small Business/Self-Employed Division (SB/SE); the IRS Wage and Investment Division (W&I); and the IRS Research, Applied Analytics, and Statistics Division (RAAS). In FY 2017, each of these IRS divisions used one or more of six data mining applications/computing environments to search for specific characteristics that are indicators of potential criminal activity:

- Investigative Data Examination Application (IDEA) - formerly known as Investigative Data Analytics;
- Lead and Case Analytics (LCA);
- Electronic Fraud Detection System (EFDS) (retired October 23, 2016);
- Return Review Program (RRP);
- FinCEN Query; and
- Compliance Data Warehouse (CDW)

IRS-CI protects IRS revenue streams by detecting fraudulent activity and preventing recurrences. In FY 2017, IRS-CI used IDEA, LCA, EFDS, and RRP systems to support this work. Data uncovered using these systems may be reflected in indictments and criminal prosecutions.

IDEA is a data query tool currently in use at the CI Lead Development Centers (LDC), Scheme Development Centers (SDC), and field offices, and it provides CI analysts and special agents the ability to quickly search electronic data through a single access point. By using the IDEA application, special agents and investigative analysts can proactively identify patterns indicative of illegal activities. This tool enhances investigation selection and supports investigative priorities in tax law enforcement, counterterrorism, and other high-priority criminal investigations. The IDEA application uses data for both reactive and proactive queries. Reactive queries are a result of specific, targeted investigations. Proactive queries are the result of pattern matching to generate leads. Data available in the IDEA application enable users to detect suspicious financial transactions indicative of money laundering, terrorism, and other financial crimes. IDEA query results are used exclusively for the purpose of generating leads. Any investigative process that results from these leads uses the corresponding data from the originating systems.

LCA is a data query and visualization application that allows CI investigative analysts and agents to query and analyze large and disparate sets of data through a single access point. This enhances the analyst's ability to develop a comprehensive picture of suspicious or criminal activity. The application presents information to the user visually, exposing associations between entities in the data that might otherwise remain undiscovered. The software used to create LCA allows users from the LDCs, SDCs, and field offices to create visualization diagrams, graphs, spreadsheets, reports, timelines, and maps to enhance investigation selection and supports investigative priorities to proactively identify and develop leads for refund fraud, identity theft, counterterrorism, money laundering, offshore abusive trust schemes, and other financial crime, as well as BSA Suspicious Activity Report (SAR) reviews and Financial Crimes Task Force activity.

IRS-CI and W&I use RRP and EFDS to maximize detection of tax return fraud, tax noncompliance, and identity theft. EFDS compiles, cross-references, and verifies information indicative of potentially fraudulent tax returns. As EFDS receives returns, it loads and assigns a score to each tax return. Scores range from 0.0 to 1.0, with a higher score indicating a greater potential for fraud. RRP expands on EFDS' capabilities by providing multiple model scores, rule breaks, and linking characteristics. In both RRP and EFDS, IRS-CI does not directly examine the scores, but does use returns that W&I determines to be potentially fraudulent as a basis for its criminal investigations.

IRS-CI and SB/SE users access the FinCEN Query system (see FinCEN report) as the system of record for BSA data.

CDW is an analytical computing environment managed by RAAS that is used by IRS researchers for high performance computing and advanced analytics. It simplifies access to over 50 legacy and third-party data sources through a self-service analytical model that fosters collaboration among business units through better sharing of data assets. Use patterns include identifying complex relationships of corporate flow-through, entity fabrication and pyramiding, and preparer interactions through the use of graph methods and network analysis; enhancing risk scores for case selection and financial crimes through the use of unstructured data, text mining, and Natural Language Processing; improving the detection of Identification (ID) theft and refund fraud patterns with statistical models and machine learning algorithms; developing new methods for embedding case routing and treatment strategies into right-time processes with dynamic, end-to-end optimization; accelerating the calculation of taxpayer burden measures, tax policy simulations, and tax gap estimates through advanced computing techniques; and rapidly integrating new IRS and third-party data for high frequency pilots.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

IDEA and LCA do not provide the IRS with the ability to determine indicators of terrorist or criminal activity. Special agents and investigative analysts can query based on experience. Agents and analysts determine indicators of fraudulent activity based on previous

successful investigations of money laundering, counterterrorism, and BSA violations.

W&I employees use RRP and EFDS to identity potentially fraudulent, noncompliant, and identity theft activity. IRS-CI uses the fraudulent tax returns identified by W&I as a basis for its criminal investigations. Paper refund returns come to EFDS from the Generalized Mainline Framework (GMF)[4] and Questionable Refund Program[5]. Paper returns come into RRP via multiple feeds from GMF. This allows W&I and SDC employees to review those returns for suspicious activities.

Prior to retirement of EFDS data mining, EFDS employed a data mining technology called IBM SPSS Modeler. Using this tool, EFDS creates rule sets using a standard built-in algorithm called C5.0. Using examples of current and prior year verified fraud and non-fraud data, the machine-learning model discerns patterns or rules indicative of fraud. The output of the model is a score where a higher score (in the range of 0.0 to 1.0) represents a higher risk or a higher likelihood of a return being fraudulent.

If a return meets designated score tolerances and other criteria, W&I and IRS-CI personnel examine the return for fraudulent activity. Once a return is verified to be false via screening, Taxpayer Protection Program authentication and/or the wage verification process, the fraudulent returns are added via EFDS systemically or by W&I and CI-IRS users to the Scheme Tracking and Retrieval System (STARS) component. IRS-CI investigative analysts review the returns in Discoverer and STARS to find possible schemes, or fraudulent patterns, which may result in a referral to a CI field office for investigation.

RRP employs multiple technologies for data mining activities. Each of these technologies uses current and prior year examples of identity theft (IDT), non-IDT tax fraud, and non-fraud to develop supervised models, unsupervised models, rules, and network analytics:

- SAS – RRP uses SAS as the workbench for developing and evaluating supervised and unsupervised models as well as for data exploration activities. RRP uses multiple SAS machine learning algorithms (e.g., decision trees, neural networks, logistic regression) to uncover patterns in the data associated with fraud. RRP also includes components of SAS' High Performing Analytics (e.g., SAS Grid, SAS in-database analytics) to develop and deploy models with greater complexity than what could be built on a traditional infrastructure. Greater complexity allows RRP models to display greater accuracy and robustness. Supervised models produce a score from 0.000 to 1.000 where a higher score represents a higher likelihood of a return being fraud.
- Greenplum Data Computing Appliance (DCA) – All RRP models are deployed and ran directly in the database. Deploying models directly to the database removes the network latency required to move data to a separate application tier server containing the models. Moreover, the Greenplum DCA provides massively parallel processing capabilities

[4] The Generalized Mainline Framework is a service center pipeline processing system that validates and perfects data from a variety of input sources. Tax returns, remittances, information returns, and adjustment and update transactions in the system are controlled, validated, corrected, and passed on for master file posting.

[5] The Questionable Refund Program (QRP) is a subsystem of EFDS. QRP is a nationwide multifunctional program designed to identify fraudulent returns, to stop the payment of fraudulent refunds, and to refer identified fraudulent refund schemes to CI field offices.

across multiple segment servers. In addition to models developed using SAS, RRP also develops models in the form of custom user-defined functions in the Greenplum DCA.

- RRP's network analytics tool – Linked Return Analysis (LRA) – uses multiple custom built Greenplum functions to link returns that display common and suspicious characteristics.
- RRP builds "identity theft filters" using Greenplum functions. These functions combine the outputs of RRP models, rules and LRA to flag suspicious cases of identity theft treatment.
- FICO Blaze Advisor (FICO BA) – RRP builds and maintains business rules using FICO BA. FICO BA provides transparency into the logic that drives business decisions. FICO BA houses the logic that drives RRP's Systemic Verification process – the rule logic that matches taxpayer submitted Income Documents (IDOCs) to the document submitted by withholding party(ies) (e.g., employer submitted W-2s containing income and withholding information).

CDW provides a state-of-the-art research and technology infrastructure to enable a full range of analytical use patterns, including large-scale analysis of historical records, distributed parallel computing of data stored across deep storage/memory architectures, and in-memory computing of large data structures, such as complex graphs. Specific analytical tools include SAS, Stata, R, Python, Neo4j, Hadoop, and Spark for statistical modeling, machine learning, graph methods, text analytics, and advanced visualization. Database technology includes SAP IQ, SAP Hana, Oracle, SQL Server, PostgreSQL, and MongoDB. CDW is a general-purpose analytical computing environment, not an application. It provides a self-service model and computing resources for users to explore and test data-driven ideas. It is not a system or application specifically designed to identify terrorist or criminal activity per se.

(C) A thorough description of the data sources that are being or will be used.

The IRS-CI applications IDEA and LCA leverage the following data sources:

- **Taxpayer:** The source is the electronically filed return, as transmitted through the Modernized E-File Program (MeF), or a paper filed tax return.
- **Employers/Payers:** Information from employers/payers captured on various forms as stored in the Information Returns Master File (IRMF).
- **Other Treasury sources:** BSA data provided by FinCEN, Specially Designated Nationals' data provided by the Office of Foreign Assets Control.
- **Other IRS sources:** Tax Exempt Organizations data, Voluntary Disclosures, Criminal Investigations data.

The EFDS and RRP application leverages the following data sources:

- **Taxpayer**: The source is the electronically filed return (as transmitted through the MeF) or a paper filed tax return. EFDS and RRP also load taxpayer data contained on the IRS Master File.
- **Employers/Payers**: Information from employers/payers captured on Form W-2 and/or Form 1099 as stored in the IRMF.

- **Other federal agencies**: Federal Bureau of Prisons for prisoner information; Social Security Administration for National Accounts Profile data for dates of births and deaths.
- **State and local agencies**: Prison systems in all states and the District of Columbia deliver prisoner-listing information annually to IRS-W&I in electronic format.

CDW leverages the following data sources:

- **Taxpayer**: Tax returns from individuals, businesses, exempt organizations, and other taxpayers as transmitted through the MeF or as a paper filed tax return.
- **Employers/Payers**: Information from employers/payers captured on various forms as stored in the Information Returns Master File (IRMF).
- **Other federal agencies:** Social Security Administration for birth/death data, Department of Justice for sealed documents, Department of Transportation for excise-related information.
- **Other IRS sources:** Tax Treaty organizations, Voluntary Disclosures, case management systems for examination, collection, and underreported data.

(D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.

The data uncovered during the query searches are only leads and require additional investigative steps for quality verification. There are no empirical data on the efficacy of searches by the IDEA and LCA applications.

The IRS retired the EFDS Data Mining component in October 2016, and it did not run in processing year 2017. Given the system did not run in 2017, there is no assessment of the system's efficacy. However, in evaluating the retirement of EFDS with RRP, the IRS considered the following metrics:

- IDT Detection: RRP protects 278 percent of the revenue value protected by EFDS-Data Mining (EFDS-DM), worth an additional $2.21 billion in annual refund revenue protection

  (In 2015, RRP and EFDS-DM MeF IDT detection ran in parallel. As of November 11, 2015, RRP selected 562,539 confirmed IDT cases ($3.45 billion in refund revenue protected) while EFDS-DM selected 194,602 confirmed IDT ($1.24 billion in refund revenue protected).)
- Non-IDT Fraud Detection: RRP protects 531 percent of the revenue value protected by EFDS-DM, worth an additional $311 million in annual refund revenue protection

  (In 2016, RRP and EFDS-DM MeF Non-IDT fraud detection – which sends returns to IVO for wage/withholding verification - ran in parallel. As of November 3, 2016, RRP selected 48,959 fraud cases ($383 million in refund revenue protected) confirmed via IVO treatment while EFDS-DM selected 14,073 fraud cases ($72.1 million in refund revenue protected) confirmed via IVO treatment.)

The efficacy of RRP can be measured in terms of identity theft detection. Two key metrics are used to assess RRP's efficacy: lead generation and True Positive Rate. In 2017(through October 11, 2017), RRP generated over 837,000 identity theft leads at a true positive rate of 53 percent.[6] This means that over 5 out of every 10 returns flagged as IDT by RRP never receive a legitimate taxpayer identity authentication via the IRS's web, phone, or in-person authentication processes. In addition to identity theft detections, RRP includes models to detect fraud that does not involve identity theft. During the year, RRP generated the following non-identity theft fraud leads (above all identity theft leads) and lead accuracy:

- RRP Non-Identity Theft Models/Filters: Over 77,000 leads at 58 percent lead accuracy;
- RRP Business Rules Filters: Over 75,000 leads at 12 percent lead accuracy; and
- RRP Frivolous Filer Rules: over 54,000 leads at 8 percent accuracy.

The efficacy of the FinCEN Query system is discussed in Section (D) of that report.

For CDW, the results produced from data analysis represent insights or potential leads and require additional investigative steps for quality verification. There is no empirical data on the efficacy of searches by these applications.

(E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

Once evidence of fraud is discovered, laws and administrative procedures, policies, and controls govern the ensuing actions. IDEA and LCA applications use PII for pattern matching, but the results of a query are used for further investigation. IRS-CI follows the IRS security and privacy Internal Revenue Manual (IRM) standards and regulations for the use and protection of PII.

The impact or likely impact of the EFDS and RRP data mining activities on privacy and civil liberties of individuals is governed by 26 U.S.C. § 6103, which provides general rules of maintaining confidentiality and permissible disclosures. Under this statute, all taxpayer data are private and confidential and protected from disclosure except under specific conditions. Additional laws provide for civil and criminal penalties for any unauthorized disclosure of taxpayer data. The penalties include (1) felony for the willful unauthorized disclosure of tax information, (2) misdemeanor for the unauthorized inspection of tax information, and (3) civil cause of action for the taxpayer whose information has been inspected or disclosed in a manner not authorized by Section 6103. The CI special agents receive periodic training on maximum sentencing and penalties for each criminal violation. Access to the system requires a background check. The IRS has a system, Online 5081, governing program access authorization.

[6] *See* IDT and IVO Performance Report 2017

Further, EFDS and RRP data mining activities, including the machine learning and scoring process, do not directly use any PII in determining whether a return is likely to be fraudulent. Scoring occurs on the characteristics of the return in question, not on the PII. When performing investigative techniques, PII associated with the return is pulled to assist in validating the return was filed using the taxpayer account in question and to determine venue of the investigation.

The tax returns that IRS-CI reviews are the subjects of criminal investigations and actions based on tax laws, policies, and criminal procedures. Other tax returns are subjected to IRS civil treatments and examination procedures that provide for due process and redress procedures through taxpayer notification, appeals, and tax court options.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

The use of all tax data is governed by 26 U.S.C. § 6103. Subsection (a) sets out the general rule of confidentiality. Subsection (b) sets forth definitions of terms commonly used throughout Section 6103. Subsections (c) through (o) of Section 6103 contain exceptions to the general rule of confidentiality. These subsections permit disclosures as described generally below:

- Section 6103(c) – Disclosures to taxpayer's designees (consent);
- Section 6103(d) – Disclosures to state tax officials and certain state and local law enforcement agencies;
- Section 6103(e) – Disclosures to the taxpayer and persons having a material interest;
- Section 6103(f) – Disclosures to certain committees of Congress;
- Section 6103(g) – Disclosures to the President and certain other persons;
- Section 6103(h) – Disclosures to Federal employees and the courts for tax administration purposes;
- Section 6103(i) – Disclosures to Federal employees for non-tax criminal law enforcement purposes and to combat terrorism, as well as the Government Accountability Office;
- Section 6103(j) – Disclosures for statistical purposes;
- Section 6103(k) – Disclosures for certain miscellaneous tax administration purposes;
- Section 6103(l) – Disclosures for purposes other than tax administration;
- Section 6103(m) – Disclosures of taxpayer identity information (generally for Federal debt collection purposes);
- Section 6103(n) – Disclosures to contractors for tax administration purposes; and
- Section 6103(o) – Disclosures with respect to certain taxes.

In addition to disclosures permitted under the provisions of Section 6103, other provisions of the Internal Revenue Code also authorize disclosure of tax information. For example, Section 6104 authorizes disclosure of certain tax information regarding tax-exempt organizations, trusts claiming charitable deductions, and qualified pension plans. Section 6110 authorizes disclosure of certain written determinations and their background files.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to:

(i) protect the privacy and due process rights of individuals, such as redress procedures; and

All tax information is protected as required in 26 U.S.C. § 6103 (see E and F above). All employees who interact with tax return and other protected information are required to undergo yearly refresher training that details their responsibilities with respect to information protection and disclosure. In addition to covering 26 U.S.C. § 6103 disclosure provisions, this training module also includes information on the Privacy Act, E-Government Act, Freedom of Information Act, and policies related to protecting PII and other sensitive information. The use of BSA information is strictly controlled under the statute that directs its collection.

The data uncovered during query in IDEA, LCA, and CDW applications are used as a lead and requires additional investigative steps to verify the quality of the information, as discussed above. IRS maintains an audit trail on all users' access to case data. In addition, a full system log is maintained for any system level activities, including new data loads to the IDEA, LCA, and CDW application.

Neither EFDS nor RRP determines whether a return is fraudulent or whether a person is going to be subject to criminal prosecution. Once fraud is suspected, laws and administrative procedures, policies, and controls govern criminal investigations or any other ensuing actions. Due process is provided during any ensuing criminal investigation or civil action.

(ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

An individual/entity self-reports tax data when submitting the information to the government. FinCEN's data are gathered from information compiled by the reporter based on information provided by their customer or based on the reporter's personal experience. Investigators scrutinize the Suspicious Activity Reports filed by the subject companies and request grand jury subpoenas for the underlying documentation. The supporting records are examined and individuals of interest are identified.

The IDEA, LCA, and CDW applications are not the authoritative owners of data. However, the data are used for investigative analysis purposes under the IRS IRM standards and guidelines. The data uncovered during query searches are only used as a lead and require additional investigative steps to verify the quality of the information. Therefore, IRS-RAAS uses these data for generating leads and the special agents verify it through further investigative or analytical work.

The CDW implements a standard set of rules during the Extract, Transformation, and Load (ETL) process to ensure that data collected from authoritative systems are accurately replicated for research purposes. These include ensuring accurate row counts, identifying duplicate rows, applying consistent data types and database indexes, and standardizing common

geographic attributes across database tables.

The tax return information and other information stored in EFDS and RRP used for data mining are based on outside data sources. The only data generated directly in EFDS are the processing steps and the results of examinations of possibly fraudulent returns. The only data generated in RRP are for system monitoring and diagnostics. Through a series of test case procedures executed through Application Qualification Testing (AQT), Systems Acceptability Testing (SAT), and Final Integration Test (FIT), the IRS verifies that the data loaded into EFDS and RRP match the data from the input source and that the system accurately displays the data in the EFDS and RRP end user applications. AQT, SAT, and FIT perform verification with each release of the system. IRS applications are required to have internal auditing capabilities. The internal audits track user access and queries performed with checks against misuse.

TTB Data Mining Activities

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

TTB's analytics program performs three types of activities that, together, qualify as data mining as defined by the Federal Agency Data Mining Reporting Act of 2007:

- Queries of commercial transactions recorded by tax and trade databases maintained by TTB and other federal agencies;
- Searches of public records and law enforcement databases for indications of illicit dealings; and
- Link analysis of connections between businesses and individuals.

TTB conducts these activities primarily for the purpose of discovering or locating patterns or anomalies indicative of activity by individuals or businesses that violate federal statutes and regulations administered by TTB. Many of the statutory provisions have criminal sanctions for their violation. The data used in these activities are, for the most part, gathered with queries of registered individuals or businesses. However, subsequent analysis of the data is primarily pattern-based, seeking anomalies in compiled records. The data mining activities also include some queries and searches that are solely pattern-based, e.g., queries of all tobacco product imports over a given time period.

The goals of TTB's data mining activities are to automate certain routine oversight processes and improve detection of common violations. These activities support predictive models and business intelligence that identify compliance risks and potential fraudulent or criminal activity that may be subject to further field review and action. TTB has models in place that score the risk of tax diversion in the tobacco industry and evaluate businesses seeking a TTB permit. TTB compiles business intelligence that highlights patterns in tax and trade data.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

TTB uses commercially available data mining technologies to access and analyze information. The experience of intelligence analysts and investigators provides the basis for determining whether a particular pattern or anomaly is indicative of violations. The ability to identify patterns and anomalies is supplemented with statistical analysis and machine learning techniques.

Most data mining is conducted with a combination of statistical analysis software (SAS) and Oracle relational database systems. Data are retrieved with SAS data step programming and/or Structured Query Language (SQL) queries. Data fields are transformed with procedures that aggregate, correlate, cluster, and otherwise simplify available variables.

Once data are collected and transformed, predictive models use the data to estimate the expected violation risk of a particular individual, business, or incident. The estimates today are based primarily on business rules and templates defined by experienced analysts. These estimates are then implemented in the SAS programming language. Patterns identified through these methods are vetted with experienced analysts and evaluated against randomized test cases.

(C) A thorough description of the data sources that are being or will be used.

TTB uses data from its own databases, the databases of other federal agencies, and commercial data providers. The data sources include:

Internal Data:

- Integrated Revenue Information System (IRIS) – tax data submitted by TTB industry members;
- Permits Online (PONL) –application data from businesses requesting a TTB permit;
- AutoAudit – data from TTB's audits and investigations;
- Formulas Online (FONL) – data from businesses submitting formula approval requests;
- COLAS Online – data from business submitting labels for approval.

External Data:

- Automated Commercial Environment (ACE)/Automated Commercial System (ACS)/Automated Export System (AES) – data regarding imports and exports of products regulated by TTB;
- Census Export Data – data regarding exports of products regulated by TTB;
- FinCEN Query – data submitted in compliance with the Bank Secrecy Act transcripts such as Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs); and
- LexisNexis Accurint – public records data of court proceedings (including some criminal cases), property holdings, licenses, and registrations. This is a fee-based service.

(D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.

TTB's data mining activity is valuable for automating certain routine oversight processes, and improving detection of compliance violations. Initial evaluations indicate that data mining enables more regular oversight and produces indicators for further field review, including investigation and audit. This evaluation is continuing and generating new improvements as the data mining activity matures.

The data mining activity, models, and business intelligence supported by the activity have been effective at helping to automate oversight processes. Predictive models automatically screen approximately 4,000 original permit applications, 2,000 active tobacco businesses, and 2,100 active distilled spirits manufacturers. The models verify information and monitor patterns in operations, tax payments, and international trade activity. The models also automatically monitor financial and trade databases for indications of activity by unregistered businesses. Automating basic screens enables TTB to provide oversight to a wider section of its regulated industries.

The ability of predictive models to detect compliance violations depends greatly on the accuracy of the source data available for the models. Data quality and mining techniques continue to improve with increased use and scrutiny over data. Predictive models that rely on data mining activity are showing promise in detecting violations. The Tobacco Importer Risk Model and Small Wine Producers Model has demonstrated accuracy of approximately 0.66 (i.e., 6 out of 10 cases recommended by these models result in the detection of previously undisclosed tax liability) and provided a positive return on investment. The accuracy rate (based on precision and recall) for the Tobacco Risk Model is approximately 0.918; the majority of leads have found compliance issues, and possible undisclosed tax liability. Evaluation of these and other models will continue as part of TTB's ongoing effort to improve model accuracy.

(E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

TTB's data mining activity has little impact on the privacy and civil liberties of individuals. Insights gained from the activity primarily result in actions against property, or the privilege to operate in regulated industries, after thorough review by experienced specialists with oversight authorities mandated by federal laws and regulations. The data sources mined are also limited to include only tax records, regulatory records, commercial records, and law enforcement records authorized for use in oversight and enforcement.

Any data concerning individuals or businesses are protected against unauthorized use

and disclosure vigorously. Policies and procedures prohibit the search of any database for reasons other than providing authorized oversight or enforcement. In cases when patterns in data are thought to be indicative of compliance issues, the data and circumstances are carefully reviewed by experienced staff before any adverse action is taken. TTB also continues to protect data against any unauthorized disclosure through all investigation and enforcement actions.

Data gathered in data mining activities is considered private and confidential, and 26 U.S.C. § 6103 protects it from disclosure. TTB handles these data consistent with that statute. Privacy protections are further assured by additional laws that provide for civil and criminal penalties for any unauthorized disclosure of taxpayer data. There are criminal penalties including: (1) felony for the willful unauthorized disclosure of tax information; (2) misdemeanor for the unauthorized inspection of tax information; and (3) civil cause of action for the taxpayer whose information has been inspected or disclosed in a manner not authorized by Section 6103.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

TTB administers the provisions of the Internal Revenue Code (IRC) relating to distilled spirits, wine, and beer (26 U.S.C. Chapter 51), tobacco (26 U.S.C. Chapter 52), firearms and ammunition excise taxes (26 U.S.C. §§ 4181, 4182, and related portions of chapter 32), and the general rules of tax procedure with respect to these commodities (including related criminal provisions at 26 U.S.C. Chapters 68 and 75). In addition, TTB administers the Federal Alcohol Administration Act (27 U.S.C. chapter 8, subchapter I), which covers basic permits, unfair trade practices, and labeling and advertising of alcohol beverages; the Alcoholic Beverage Labeling Act of 1988 (27 U.S.C. chapter 8, subchapter II), which requires a specific "Government Warning" statement on alcohol beverage labels; and the Webb-Kenyon Act (27 U.S.C. §§ 122-122b), which prohibits the shipment of liquor into a state in violation of state law.

The IRC establishes qualification criteria to engage in the businesses relating to manufacturing and importing or exporting tobacco products, and manufacturing or importing processed tobacco, and require that persons obtain permits to engage in these activities. *See* 26 U.S.C. § 5713. A permit qualification requirement also applies to the production of distilled spirits and wine, as well as to the wholesaling and importation of all beverage alcohol products. *See* 26 U.S.C. §§ 5171(c) and (d), 5271; *see also* 27 U.S.C. § 201 *et seq*.

Through an agreement dated May 3, 2005, FinCEN granted TTB direct electronic access to data collected pursuant to provisions of the Bank Secrecy Act, 31 U.S.C. § 5311 *et seq*. The direct access is for tax and regulatory purposes relevant to TTB's mission.

The Secretary of the Treasury retained authority to collect excise taxes on imported alcohol and tobacco products through the Homeland Security Act of 2002. *See* 6 U.S.C. §§ 212 and 215. Through Treasury Order 100–16, the Secretary of the Treasury delegates authority over "Customs revenue functions" to the Secretary of the Department of Homeland Security. The Homeland Security Act of 2002 defines these functions as "assessing and collecting customs duties (including antidumping and countervailing duties and duties imposed under

safeguard provisions), excise taxes, fees, and penalties due on imported merchandise, including classifying and valuing merchandise for purposes of such assessment." 6 U.S.C. § 215(a)(1).

The Homeland Security Act of 2002, Pub. L. No. 107-296; Executive Order 13439, July 18, 2007; the Internal Revenue Code of 1986 (IRC); and the Federal Alcohol Administration Act, 27 U.S.C. chapter 8 (FAA Act) authorize TTB to access data within Customs and Border Protection (CBP) data systems, as necessary to fulfill TTB's statutory mission. TTB is working in conjunction with CBP to fulfill its statutory mission as it relates to imported products subject to various taxes and to ensure taxpayers understand their tax responsibilities related to these products. Cooperative efforts across federal agency lines will accommodate the collection of data as it relates to imported commodities subject to federal taxes, including but not limited to retail, excise, manufacturers, and environmental taxes.

When the data analyzed by the models consist of taxpayer information, 26 U.S.C. § 6103 governs its use. Subsection (a) sets out the general rule of confidentiality. Subsection (b) sets forth definitions of terms commonly used throughout Section 6103.

Subsections (c) through (o) of Section 6103 contain exceptions to the general rule of confidentiality. The use of confidential commercial, financial, or trade secrets information is governed by the Trade Secrets Act, 18 U.S.C. § 1905, which prohibits the unlawful disclosure of this information by any federal official, employee, or contractor.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to:

(i) protect the privacy and due process rights of individuals, such as redress procedures; and

All of TTB's information collections are subject to OMB review process and any forms that request personal information include a Privacy Act Statement. In addition, TTB's privacy policy is posted on TTB's website and is referenced on TTB's Online Applications. TTB's systems of record notice can be found in the Federal Register on January 28, 2015 (80 FR 4637).

TTB data mining activities do not determine whether a person or entity will be subject to administrative enforcement action or criminal prosecution. Any audit or investigation that is initiated based, in part, upon data from the activities are governed by the laws, administrative procedures, policies, and controls that govern criminal investigations or any other ensuing actions.

Information generated and accessed by the data mining activities is protected by internal controls that limit access to persons whose official duties require inspection of such information for tax administration purposes. The information is further protected by 26 U.S.C. § 6103, governing the confidentiality of returns and return information, and the Trade Secrets Act, 18 U.S.C. § 1905, which protects confidential commercial, financial, or trade secrets information collected by the federal government.

TTB notifies system operators of the requirements and legal consequences of accessing predictive models in production. The message states:

> 26 U.S.C. 6103 Data Warning. Information contained in this report is tax return information protected from disclosure by 26 U.S.C. 6103. By accessing this report, you hereby certify that your official duties require you to inspect such information for tax administration purposes.

Users of predictive models in production receive training in the proper handling of information. Users receive system demonstrations of the model and have access to a user guide. The same process will be followed for future models when successful testing and evaluation has been completed. Field Operations staff receive 26 U.S.C. § 6103 and disclosure training. In addition, all TTB employees complete the annual Privacy Awareness and Cyber Security Awareness training. Finally, system sponsors and IT staff supporting development, maintenance, and operations of IT systems are required to take additional specialized security training each year.

(ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

The data mining activities rely on information collected through systems that have their own accuracy related checks and balances. TTB does not rely solely on information gathered through predictive models to take any adverse action against any individual or entity. Rather, the models are the first step in gathering data and this information is verified through subsequent research and audits of companies and importers before any adverse action is taken.

TTB documents and manages all data sets associated with its systems using the TTB Systems Development Life Cycle (SDLC). Checks and balances are inherent to the data correction process ensuring different teams handle different steps of the effort and include oversight by the Office of the Chief Information Officer Quality Assurance (OCIO QA) Team. When the system owner identifies inconsistencies with data, TTB's OCIO QA Team may initiate a data correction. All changes are documented via the Request for Change process managed by the Configuration Management Team and work orders track the correction through its lifecycle (from request to development and through implementation), which includes confirmation of successful completion by the system owner. The process includes specific identification of the data to be corrected along with rationale for the change. SDLC artifacts (e.g., database scripts) supporting data corrections conform to Data Management (DM) standards. The Software Maintenance Team verifies analysis, development, and testing through a quality review process conducted by the DM Team to ensure the data correction is thoroughly documented. Once the DM Team has approved the data correction, the Operations Team executes the correction and the system owner verifies the correction.

The Memorandum of Understanding with CBP contains language that both parties will notify one another if either agency discovers data issues. Also, the ACS and ACE data import processes in support of the Tobacco Importer Risk Model were documented and tested using TTB's SDLC. For all available governmental data sources, users must sign a non-disclosure

agreement before receiving access.

FinCEN Data Mining Activities

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. To accomplish its mission, FinCEN provides financial intelligence, data stewardship, and support for law enforcement, the intelligence community, and our foreign Financial Intelligence Unit (FIU) partners. FinCEN also engages in the detection of trends and typologies of money laundering and terror finance. FinCEN strives to respect privacy, civil rights and the exercise of civil liberties while overseeing the data it maintains and uses in fulfillment of its mission as set forth under the USA PATRIOT Act, Pub. L. No. 107-56.

In furtherance of this goal, as set forth in 31 U.S.C. § 310, FinCEN is required to maintain a government-wide data access service with a range of financial transaction information; to conduct analysis and dissemination of information in support of law enforcement at the federal, state, local, and international levels; to identify emerging trends and methods in money laundering and other financial crimes; to serve as the FIU of the United States; and to carry out other delegated regulatory responsibilities. FinCEN works to achieve its mission while avoiding the collection and indexing of information on persons exercising their constitutional rights and civil liberties.

FinCEN's analysts use various data analysis techniques for generating leads on subjects or institutions whose activities warrant outreach, investigation, or other statutorily mandated activities.

FinCEN has successfully developed algorithms to identify transactions associated with specific types of financial crimes, such as funnel account activity[7] related to transnational organized crime groups. FinCEN also uses algorithms to examine filing patterns across financial sectors. This analysis supports a broad range of objectives from the identification of trends and patterns of illicit financial activity to the detection of institutions that may require additional regulatory oversight.

FinCEN continues to develop and expand the use of automated business rules to rapidly identify high value reports of illicit financial activity on a daily basis. The term "business rule" refers to automated queries or algorithms designed to screen incoming BSA filings against established criteria to identify high priority filings likely to require further review or analysis. Rule findings are reviewed internally by FinCEN and distributed to external stakeholders, such

[7] FinCEN defines a "funnel account" as an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.

as law enforcement and FIU partners. FinCEN's business rules play a vital role in the identification and dissemination of timely financial intelligence to combat threats such as terrorist financing, money laundering, cyber threats, and other illicit financial activity.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

FinCEN leverages two principal methods for deriving information relevant to illicit financial activity from the BSA data. The first is content driven, that is, searching for specific entity names, or term combinations used in reporting that are associated with various types of illicit financial activity. The second method is pattern driven and can take various forms. Patterns may be derived from searches for a particular type of subject in the data. FinCEN then identifies subjects that fit that same pattern and have certain filing profiles. Matching filing patterns across different types of BSA reports highlights anomalous behavior that leads to the identification of subjects for potential investigation.

For content driven data analysis, FinCEN staff use a web-based application called FinCEN Query. This application provides analysts with the capability to search for specific entity names and term combinations across all of FinCEN's records. For pattern driven analysis, staff uses FinCEN's "Advanced Analytics" system. This system is comprised of commercial off-the-shelf (COTS) and custom developed tools with capabilities including statistical, social network, and geospatial analysis, data modelling and visualization, and text analytics that aid in the analysis of BSA data.

(C) A thorough description of the data sources that are being or will be used.

BSA reports administered by FinCEN, e.g., a report by a financial institution of a suspicious transaction relevant to a possible violation of law or regulation,[8] form the underlying data for FinCEN's manual and automated search methods and trend analysis activities.

To accomplish its mission and give context to the data FinCEN extracts from its BSA database, FinCEN must consider other information available to it through a variety of sources, including open source material, law enforcement information, other government information, and information obtained through subscription services. This information is used to support or amplify conclusions or hypotheses derived from the analysis of BSA data. For example, commercially available databases are used to support or further identify information and to aid in the identification of potential illicit activity based on suspicious trends, patterns, or methods. FinCEN's trend analysis uses any records available to it in fulfilling its mission, including subpoenaed financial records, public source information, commercial database information, and

[8] 31 U.S.C. § 5318(g).

third-party data sources, such as Census Bureau, Social Security Administration,[9] and Office of Foreign Assets Control data.

(D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.

FinCEN provides strategic and tactical products for several audiences: law enforcement, foreign FIU partners, financial regulators, the financial industry, and the general public. Each of these sets of consumers has different restrictions or guidelines under which FinCEN can provide BSA data or BSA data derived analysis.

In FY 2017, FinCEN produced a total of 1,415 financial intelligence products for law enforcement partners and responded to 828 requests for BSA information from foreign FIU partners. For domestic and foreign law enforcement partners, FinCEN provides high value data analytics. FinCEN annually receives the results of surveys of its foreign Egmont[10] member counterparts and domestic law enforcement agencies regarding the utility of its analytical products. These survey results consistently reflect positive feedback from our foreign and domestic stakeholders. FinCEN also receives feedback on individual reports from law enforcement and regulatory agencies on our efforts to combat terrorism financing, healthcare, mortgage, and government programs fraud, southwest border narcotics, and bulk cash smuggling. Examples of several analytical projects that received significant positive feedback are outlined below:

- To combat terrorist financing threats, FinCEN has developed more than 35 business rules designed to identify and disrupt terrorist organizations' revenue streams and target their financial support networks. The rules generate more than 2,675 leads per month that FinCEN disseminates to the law enforcement, intelligence, and FIU communities via expedited "Flash Reports." Flash Reports are designed to provide critical financial intelligence to FinCEN's stakeholders on a timely basis. Since the inception of the Flash Reporting program in late 2014, FinCEN has disseminated more than 2,600 terrorism-related Flash Reports. Feedback on these reports has been extremely positive, with stakeholders noting that the reports helped corroborate information related to investigations, provided new leads, and assisted investigators in identifying targets.

[9] The Death Master File is Social Security Administration (SSA) information used by medical researchers, hospitals, medical programs, and law enforcement agencies and other government agencies to verify a person's death and to prevent fraud. Although it is SSA information, the National Technical Information Service in the Department of Commerce maintains the database. For more data, please visit the NTIS website.

[10] The Egmont Group is a united body of 156 Financial Intelligence Units (FIUs). The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF).

- As part of those 35 rules, FinCEN has implemented a series of cybercrime-related business rules to address emerging cyber threats and identify potential vulnerabilities to financial institutions. FinCEN leverages business rules to actively monitor the volume of reported cyber threats, evaluate the potential risk these threats pose to financial institutions, and identify opportunities to increase threat preparedness. FinCEN has successfully leveraged cyber-related rules to track cyber criminals and develop financial intelligence products for law enforcement, identify the use of specialized malware associated with large-scale breaches and targeted attacks on payment systems, as well as review reporting of malware signatures and cyber intrusions affecting financial institutions.

- To proactively combat significant money laundering and terrorist financing threats, FinCEN has implemented a series of algorithms designed to identify those filers that have the largest volume of Suspicious Activity Report (SAR) filings (both in number of filings and/or suspicious activity amounts) that have not already been identified by law enforcement. The algorithms are designed to aggregate data on individuals and businesses within the BSA who may be intentionally using aliases and identifiers to obfuscate their identities. The algorithms have been instrumental in generating high priority leads for FinCEN's Intelligence Division.

FinCEN narrowly tailors its business rules to achieve its mission, and each rule is developed, tested, implemented, and re-tested for efficacy throughout its deployment. The Office of Chief Counsel and the Technology Division are engaged during the development of all business rules. FinCEN continues to receive strong positive feedback both from our domestic and international partners on the value of the financial intelligence derived from our business rules program.

Finally, FinCEN provides annual aggregated statistics on SAR data by sector to the public in a publication titled "SAR Stats" and provides an interactive SAR Stats module for SAR statistical data searches. The most recent version of SAR Stats was published on FinCEN's website in March 2017. Readers accessed the publication an average of 53,000 times per month w/ approximately 1,600 daily users in 2017 – an increase of 76% and 60%, respectively, from the year prior. Since going live in March 2015, Interactive SAR Stats has received 1,089,730 access hits, an indication of the data's high utility.

(E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

The impact of FinCEN's congressionally mandated mission on the privacy and civil liberties expectations of individuals has been and will continue to be minimal. As a threshold matter, the Supreme Court has ruled that individuals have no constitutionally protected "expectation of privacy" in the financial information that banks and other financial institutions hold, and that FinCEN collects and analyzes pursuant to its authority in 31 U.S.C. § 310 and the BSA (discussed in more detail in item (F) below). Moreover, the Right to Financial Privacy Act

of 1978[11] expressly states that it provides no protection for financial records or information required to be reported in accordance with any federal statute or regulation, which includes information contained in BSA reports.[12] Nevertheless, during the development of all business rules, analytical models, and algorithms, FinCEN considers whether the analytics will adversely affect an individual or entity's (to the extent applicable) privacy, civil rights, or civil liberties.

Significantly, FinCEN takes no adverse actions against individuals based solely on the existence of, or information contained in, BSA data. Since a BSA report itself is not necessarily indicative of criminal activity, it is only useful when viewed in conjunction with other evidence. Therefore, in addition to considering it along with other information when taking actions under its own authorities, FinCEN provides the data, or analytical products analyzing the data, to outside agencies where the information may be relevant to current or potential investigations or proceedings under the jurisdiction of those agencies.

The collected information is generally subject to the Privacy Act of 1974,[13] discussed in more detail under item (F) below. FinCEN has developed extensive policies and procedures to ensure, to the extent reasonably possible, that: (1) the analyzed information is used for purposes authorized by applicable law; and (2) the security of the information is adequately maintained. Analytical products produced by FinCEN are subject to clearly specified restrictions regarding use and further dissemination of the products to ensure that the products will only be used by appropriate agencies for statutorily authorized purposes. To the extent such products reference information collected pursuant to the BSA, FinCEN has issued guidelines requiring user agencies to attach warning language to such products and to follow specific procedures for further dissemination of the BSA information. These procedures aim to ensure that: (1) only appropriate agencies will have access to the information; (2) the information will be used for statutorily authorized purposes; (3) agencies with access to FinCEN data are aware of the sensitivity of the material; and (4) FinCEN will be able to track which agencies have such materials in their possession.

FinCEN posts PIAs on its public website, which informs the public of FinCEN's activities and practices related to the collection, processing, retention, and distribution of PII.[14] The PII that FinCEN data repositories handle is necessary to assist regulators and law enforcement in identifying and monitoring the financial activities of individuals who are potentially committing financial crimes.

---

[11] 12 U.S.C. § 3401, *et seq*.

[12] 12 U.S.C. § 3413(d) ("Disclosure pursuant to Federal statute or rule promulgated thereunder nothing in this chapter shall authorize the withholding of financial records or information required to be reported in accordance with any Federal statute or rule promulgated thereunder.")

[13] 5 U.S.C. § 552a.

[14] For more information about FinCEN PIAs, please visit FinCEN's website.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

1) The Bank Secrecy Act, 31 U.S.C. § 5311, et seq. (BSA) and Implementing Regulations, 31 C.F.R. Chapter X, et seq:

31 U.S.C. § 5311— Declaration of Purpose

This section specifies that the purpose of the recordkeeping and reporting requirements in the BSA is to, "require certain reports where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." FinCEN strives to ensure that all uses of information are consistent with this purpose.

31 C.F.R. § 1010.301 — Determination by the Secretary

This regulation provides the determination that the reports collected pursuant to the BSA have a, "high degree of usefulness," in criminal, tax, or regulatory investigations or proceedings.

31 U.S.C. § 5319 — Availability of Reports

This section makes it clear that, upon request, the Secretary of the Treasury (as delegated to FinCEN pursuant to Treasury Order 180-01) shall provide BSA information to an agency, including state financial institutions supervisory agencies, United States intelligence agencies, or self-regulatory organizations registered with the Securities and Exchange Commission or the Commodity Futures Trading Commission, for purposes consistent with the subsection. This section also provides that reports collected pursuant to the BSA are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. § 552.

31 C.F.R. § 1010.950 — Availability of Information

This section authorizes the Secretary to disclose BSA information for any reason consistent with the purposes of the BSA, and specifies that the recipients are to receive the information in confidence and shall not be further disclosed to any person except for official purposes relating to the investigation, proceeding or matter in connection with which the information is sought.

31 U.S.C. § 5313 — Reports on domestic coins and currency transactions

This section provides for the reporting by financial institutions of reports of certain currency transactions in an amount, denomination, or amount and denomination, or under circumstances the Secretary (as delegated to FinCEN) prescribes by regulation.

31 C.F.R. §§ 1010.311; 1021.311 — Reports of transactions in currency

These regulations implement the reporting requirement of 31 U.S.C. § 5313 and specify the amount of reportable transactions in currency at more than $10,000.

31 U.S.C. § 5316 — Reports on exporting and importing monetary instruments

This section requires reports by those that transport currency or other monetary instruments of more than $10,000 at one time from or through a place outside the United States into the United States, or from the United States to or through a place outside the United States.

31 C.F.R. § 1010.340 — Reports of transportation of currency or monetary instruments

This regulation implements the reporting requirement of 31 U.S.C. § 5316 with respect to currency or other monetary instruments of more than $10,000 physically transported, mailed, or shipped into the United States or physically transported, mailed, or shipped outside the United States.

31 U.S.C. § 5314 — Records and reports on foreign financial agency transactions

This section authorizes the Secretary (as delegated to FinCEN) to prescribe regulations requiring the reporting of certain types of foreign transactions and relationships with foreign financial institutions.

31 C.F.R. § 1010.350 — Reports of foreign financial accounts

This regulation, implementing 31 U.S.C. § 5314, requires that U.S. persons file reports of foreign bank accounts.

31 C.F.R. § 1010.360 – Reports of transactions with foreign financial agencies

This regulation provides that the Secretary (as delegated to FinCEN) may promulgate regulations requiring specified financial institutions to file reports of certain transactions with designated foreign financial agencies. These regulations may be kept confidential, and do not always have to be published in the Federal Register, so long as any financial institutions subject to the regulation will be named and personally served or otherwise given actual notice.

31 U.S.C. § 5318(g) — Reporting of suspicious transactions

This section authorizes the Secretary (as delegated to FinCEN), to require the reporting of suspicious transactions relevant to a possible violation of law or regulation. The section also provides for the confidentiality of such reports, barring financial institutions from notifying anyone involved in the transaction that the transaction has been reported. Government employees are subject to the same confidentiality restrictions, except as "necessary to fulfill the official duties" of such employees. The policies and procedures detailed above in response to item (E) are aimed, in large part, at maintaining the confidentiality of these reports.

31 C.F.R. §§1010.320; 1020.320; 1021.320; 1022.320; 1023.320; 1024.320; 1025.320; 1026.320 — Reports of Suspicious Transactions

These regulations implement 31 U.S.C. § 5318(g), requiring covered financial institutions to file suspicious activity reports and requiring the maintaining of strict confidentiality of the reports.

31 U.S.C. § 5331 — Reports relating to coins and currency received in nonfinancial trade or business

This section provides for the reporting of currency transactions of more than $10,000 by businesses other than financial institutions.

31 C.F.R. § 1010.330 — Reports related to currency in excess of $10,000 received in a trade or business

This regulation implements 31 U.S.C. § 5331.

12 U.S.C. § 1829b (b)(3) – International Funds Transfer Reporting Requirements

This section states that the Secretary and the Board shall jointly prescribe, after consultation with State banking supervisors, final regulations requiring that insured depository institutions, businesses that provide check cashing services, money transmitting businesses, and businesses that issue or redeem money orders, travelers' checks or other similar instruments maintain such records of payment orders which involve international transactions; and direct transfers of funds over wholesale funds transfer systems or on the books of any insured depository institution, or on the books of any business that provides check cashing services, any money transmitting business, and any business that issues or redeems money orders, travelers' checks or similar instruments, that will have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.

31 CFR § 1020.410(a) – Records to be made and retained by banks

This regulation implements 12 U.S.C. § 1829b (b)(3), and requires each bank covered by the regulation to retain records of funds transfers in the amount of $3,000 or more.

31 U.S.C. § 5318A – Special measures for jurisdictions, financial institutions, international transactions, or types of accounts of primary money laundering concern

Upon making a finding that a jurisdiction outside of the United States, one or more financial institutions operating outside of the United States, one or more classes of transactions within, or involving, a jurisdiction outside of the United States, or one or more types of accounts is of primary money laundering concern, the Secretary of the Treasury (as delegated to FinCEN) may require any domestic financial institution or financial agency to maintain records, file reports, or both, concerning the aggregate amount of transactions, or concerning each transaction, with respect to the entity found to be of primary money laundering concern;

beneficial ownership of any account opened or maintained in the United States by a foreign person or a representative of that foreign person that involves the entity found to be of primary money laundering concern; or information relating to certain correspondent accounts.

Section 314a of the USA PATRIOT Act – Cooperative Efforts to Deter Money Laundering

This section (located in the Historical and Statutory Notes to 31 U.S.C. § 5311) helps law enforcement identify, disrupt, and prevent terrorist acts and money laundering activities by encouraging further cooperation among law enforcement, regulators, and financial institutions to share information regarding those suspected of being involved in terrorism or money laundering.

31 CFR § 1010.520 – Information sharing between government agencies and financial institutions

This regulation implements Section 314a of the USA PATRIOT Act and provides that a law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on the investigating agency's behalf, certain information from a financial institutions or group of financial institutions. The requesting agency must provide a written certification that each entity for which the agency is seeking information is engaged in, or is reasonably suspected based on credible evidence of engaging in, terrorist activity or money laundering along with specific identifies. FinCEN may also solicit, on its own behalf, and on behalf of appropriate components of the Department of the Treasury such information.

2) The Privacy Act of 1974 (Privacy Act), 5 U.S.C. § 552a

Generally, the Privacy Act protects reports that FinCEN collects pursuant to the BSA as these reports are "records" contained in a "system of records."[15] The Privacy Act provides that covered records may be disclosed without the permission of the individual to whom the record pertains if they are disclosed pursuant to a "routine use."[16] FinCEN includes sets of routine uses in its published Systems of Records Notices (SORNs) as the Privacy Act requires. These routine uses identify the individuals and organizations external to the U.S. Department of the Treasury with which FinCEN routinely shares BSA information. Sharing with these specified recipients is consistent with the purposes for which the information is collected, as specified in the BSA.

FinCEN has three SORNs that cover the information it collects under the BSA:

[15] 5 U.S.C. § 552a(a)(3) (defining a "record" to mean any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph and a "system of records" to mean a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular a

[16] 5 U.S.C. § 552a(b)(3).

(1) Treasury/FinCEN .001, *FinCEN Investigations and Examinations System*;[17]
(2) Treasury/FinCEN .002, *Suspicious Activity Report (SAR) System*;[18] and,
(3) Treasury/FinCEN .003, *Bank Secrecy Act (BSA) Reports System*.[19]

FinCEN followed Privacy Act procedures (including appropriate public notice and comment periods) to exempt certain records maintained in the SARs and BSA systems of records from specific provisions of the Privacy Act, including those allowing for subject's access to the reports, notification to the subject when reports are shared, requests for correction of the contents of such reports by the subject, and the civil remedies covering these areas. These exemptions prevent individuals who are planning crimes from avoiding detection or apprehension or structuring their operations to avoid detection or apprehension.

3) Other Relevant Provisions

31 U.S.C. § 310— Financial Crimes Enforcement Network

This section establishes FinCEN as a bureau in the Department of the Treasury, sets out the duties and powers of the Director, and empowers the Director to administer the BSA to the extent delegated by the Secretary of the Treasury.[20] This section also requires FinCEN to maintain a "government-wide data access service" for the information collected under the BSA, as well as records and data maintained by other government agencies and other publicly and privately available information.[21]

FinCEN is required to "analyze and disseminate" the data for a broad range of purposes consistent with the law.[22] These purposes include identifying possible criminal activity; supporting domestic and international criminal investigations (and related civil proceedings); determining emerging trends and methods in money laundering and other financial crimes; supporting the conduct of intelligence and counterintelligence activities, including analysis, to protect against international terrorism; and supporting government initiatives against money laundering.

The section further requires that FinCEN furnish research, analytical, and informational services to financial institutions and domestic and foreign law enforcement agencies for the "detection, prevention, and prosecution of terrorism, organized crime, money laundering and other financial crimes," and provide, "computer and data support and data analysis to the Secretary of the Treasury for tracking and controlling foreign assets."[23] The section also provides for the establishment of standards for making the information available through

[17] 79 Fed. Reg. 20969 (April 14, 2014).
[18] *Id*. at 20972.
[19] *Id*. at 20974.
[20] Treasury Order 180-01, *Financial Crimes Enforcement Network* (July 1, 2014) (delegating to the Director of FinCEN various duties and responsibilities, including the authority to administer, implement, and enforce the BSA).
[21] 31 U.S.C.§ 310(b)(2)(B).
[22] *Id*. at § 310(b)(2)(C)(i)-(vii).
[23] *Id*. at § 310(b)(2)(E), (G).

efficient means, and to screen appropriate users and appropriate uses.[24] The activities and procedures described in this report adhere to the requirements of this statute.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to:

(i) protect the privacy and due process rights of individuals, such as redress procedures; and

A description of the policies, procedures, and guidance in place to ensure the privacy and due process rights of individuals that are the subject of FinCEN data mining activities is provided in subsection (E) above.

(ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

FinCEN, through its data perfection procedures, ensures that information contained in the database of BSA reports is accurate and complete. In addition, as discussed in item (E) above, FinCEN does not take adverse actions against individuals (outside the context of enforcing the requirements of the BSA itself) based on the information contained in BSA reports. In addition, because user agencies only use BSA information in conjunction with other evidence, a BSA report in itself is not used as the sole basis for adverse actions by user agencies. Accordingly, there is an inherent system of "checks and balances" in the use of BSA information that greatly reduces the risk of harmful consequences from inaccuracies that may be contained in BSA reports.

As noted earlier in this report, individuals have no constitutionally protected "expectation of privacy" in FinCEN's BSA data users takes no adverse actions against individuals based on the BSA data collected. Nevertheless, FinCEN's BSA analyst training discusses the importance of confidentiality, safeguarding and non-disclosure of BSA data to unauthorized individuals or organizations. Additionally, all FinCEN staff are required to complete Privacy Awareness training annually that includes an explanation of the staff's civil liberties and privacy responsibilities, including the Privacy Act handling and safeguarding responsibilities that apply to all BSA data. Accountability for the security and confidentiality of the BSA data and its handling are prominently articulated in all course materials. FinCEN also has mandatory training for its BSA data users that includes secure handling and safeguarding of the information. FinCEN provides online training for all external users as a requirement for access to FinCEN Query. Biennially, at a minimum, BSA data users must complete training as a requirement of continued system access. In addition to this online training, FinCEN hosts webinars as requested.

[24] *Id*. at § 310(c)(1) and (c)(2).

SECTION THREE: DEPARTMENT OF THE TREASURY SEMIANNUAL 2017 REPORTING ON PRIVACY AND CIVIL LIBERTIES ACTIVITIES PURSUANT TO SECTION 803 OF THE IMPLEMENTATING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007
FOR REPORTING PERIOD APRIL 1, 2017 TO SEPTEMBER 30, 2017

1. Introduction

The Assistant Secretary for Management (ASM) is the Department of the Treasury's (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 (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 (PTR) and provides the ASM with day-to-day support in executing his PCLO duties.

Section 803 of the 9/11 Commission Act, 42 U.S.C. § 2000ee-1, 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.

(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.

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 (PCLIA) as required by the E-Government Act of 2002;[25]
c) System of Records Notices, as required by the Privacy Act and any associated Final Rules for Privacy Act exemptions;[26]
d) Privacy Act Statements, as required under the Privacy Act,[27] to provide notice to individuals at the point of collection;
e) Computer Matching Agreements, as required by the Privacy Act;[28]
f) Data Mining Reports, as required by Section 804 of the 9/11 Commission Act of 2007;[29]
g) Privacy Compliance Reviews;
h) Privacy reviews of IT and program budget requests, including Office of Management and Budget Exhibit 300s and Enterprise Architecture Alignment Requests through the Department of Homeland Security Enterprise Architecture Board; 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,

[25] 44 U.S.C. § 3501 note.
[26] 5 U.S.C. § 552a(j),(k).
[27] 5 U.S.C. § 552a(e)(3).
[28] 42 U.S.C. § 2000ee-3.
[29] 6 U.S.C. § 142.

Treasury published 69 new, updated, or renewed PCLIAs. All published Treasury PCLIAs are available at: http://www.treasury.gov/privacy/PIAs/Pages/default.aspx. One example of a new PCLIA is summarized below:

On June 30, 2017, the IRS published a PCLIA for the eAuthentication Data Extract, Research Analytics, and Applied Statistics EDA. The eAuthentication Data Extract is a system which allows a taxpayer to validate his or her identity and create an online account to access other IRS products. This PCLIA relates to the analysis of the data extract of multiple daily reconciliation files sent by Equifax to authenticate data and account usage data obtained from IRS Cybersecurity during the reporting period. The purpose of this analysis is to assess the accuracy of the authentication product and to detect potentially fraudulent behavior after the point of authentication.

The results of the analysis will inform improvements to the authentication product configuration as well as help detect any account compromise after authentication. The data will also be used in a cross-channel analysis of all relevant authentication techniques. This cross-channel analysis will allow the IRS to have a holistic understanding of the accuracy of all authentication techniques enabling both near/long term improvements in authentication accuracy as well as detection/mitigation of potentially fraudulent account access.

4. System of Records Notices

During the reporting period, Treasury published and updated one SORN. All Treasury SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act Exemptions are available at: http://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 our website or the Federal Register for the full text of our SORNs.

Treasury's Bureau of Engraving and Printing (BEP) modified one existing SORN during the reporting period. BEP .046, Automated Mutilated Currency Tracking System tracks requests for examination of mutilated currency submitted by individuals, institutions, or executors/ administrators ("requestors') to the BEP for evaluation and possible redemption. On March 29, 2014, BEP amended subpart B of 31 CFR Part 100, which covers the exchange of mutilated currency in order to update the mutilated currency procedures and eliminate references to obsolete practices and terms. The goal of these amendments is to deter fraud and abuse in the mutilated currency redemption process. These amendments are needed for the existing system of records to properly identify the individuals submitting the request, document how the currency came to be mutilated, provide bank account information to Treasury's Bureau of the Fiscal Service to allow payment via electronic funds transfers, and help deter fraud and abuse in mutilated currency submissions. This updated system of records was last published on August 9, 2017, at 82 FR 37291.

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 Program Agreements are available at: https://www.treasury.gov/privacy/Computer-Matching-Programs/Pages/default.aspx.

During the reporting period, the Data Integrity Board reviewed and approved four 12-month renewals and two 18-month re-establishment agreements. Below are a few examples of these computer matching programs:

a) The Bureau of the Fiscal Service and the Social Security Administration (SSA) matching program allows FS to disclose ownership of savings securities to SSA. This information is essential in verifying an individual's self-certification of his or her financial status used to determine eligibility for low-income subsidy assistance in the Medicare Part D prescription drug benefit program. On September 11, 2017, Treasury approved a 12-month renewal of the matching program, effective September 30, 2017. The original agreement is available at 81 FR 9921.
b) The IRS and 53 state agencies, SSA, Veterans Benefits Administration (VBA), and Veterans Health Administration (VHA) matching program allows the IRS to disclose certain return information to the 53 state agencies, SSA, VBA, and VHA. This information is used for verifying eligibility for, and the correct amount of, benefits for individuals applying for or receiving benefits under state administered programs covered by this agreement. On May 18, 2017, Treasury approved a 12-month renewal of the matching program, effective July 1, 2017. The original agreement is available at 80 FR 59245.
c) The IRS and SSA matching program allows the IRS to disclose certain information to the SSA for the purpose of verifying eligibility for the Prescription Drug Subsidy Program and determining the correct subsidy percentage of benefits being received. On September 1, 2017, Treasury approved an 18-month re-establishment of the matching program, effective November 11, 2017. The original agreement is available 80 FR 18673.

6. Privacy Compliance Reviews

Treasury conducts Privacy Compliance Reviews (PCR) 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 (PO) took a proactive approach to privacy policy development by monitoring emerging issues, identifying gaps, issuing policy,

and establishing accountability. In 2017, the IRS issued Interim Guidance on "Digital Assistants and Other Devices," which provides specific policy regarding methods for protecting privacy when working around digital assistants and other devices that can record and/or transmit sensitive audio or visual information in the work/telework environment.

Furthermore, the IRS continues its effort in rolling out the Taxpayer Digital Communication (TDC), which provides secure methods for the IRS to communicate with individuals. Currently, only certain notices are sent via TDC. The IRS continues to work with business units on these solutions, to ensure all privacy issues are considered and addressed.

The IRS also interacted with vendors to deploy a taxpayer authentication pilot. The work was performed on a no-fee trial services which is a non-formal contract negotiation and can create potential privacy issues. The IRS is addressing these "no-fee" interactions and standardizing their process in these instances to ensure data is not used outside the services provided and all other privacy concerns are addressed in Memoranda of Understanding or Bailment Agreements.

Lastly, 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. During the reporting period, Treasury conducted a review in response to the SSN Fraud Prevention Act of 2017 and identified all Treasury forms that require SSNs and are sent through the mail. The information was compiled during the reporting period, but the response to Congress was submitted outside the reporting period and will be addressed in the next 803 report covering the period of October 1, 2017 to March 31, 2018. During the next reporting period, Treasury will conduct 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.

7. Advice and Responses

Treasury provides privacy advice throughout the year to its bureaus and offices. Two examples of guidance are included below:

a. The Departmental Offices provided the following advice and recommendations in compliance with the Privacy Act of 1974, 5 U.S.C. § 552a, and the operational and privacy-specific safeguards outlined in the NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

    - Notified users on issues related to the collection and use of their PII and obtain their explicit consent before proceeding with the deployment of a new or modified system.
    - Update applicable policies, procedures and Rules of Behavior for protecting the confidentiality of PII.
    - Conducted an analysis of de-identified data elements which posed a risk of re-identification.

b. The Special Inspector for the Troubled Asset Relief Program (SIGTARP) provided the following advice and guidance related to disclosing PII while protecting its confidentiality in accordance with the NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act*.
    - Anonymize information prior to disclosure to reduce risk. This is information which was previously identifiable and has now been de-identified.
    - The disclosure was identified as a routine use in the applicable SIGTARP SORN and was permissible under the provisions of the Privacy Act.

In each of the situations described above, the advice was accepted and acted upon as required.

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, Pub. L. No. 113-126 (July 7, 2014), this semiannual report summarizes Treasury's privacy activities from April 1, 2017, through September 30, 2017. Treasury will continue to work with the Congress, colleagues in other federal departments and agencies, and the public to protect privacy in all of our efforts.

Report Conclusion

The Department of the Treasury is pleased to provide to Congress its Annual Privacy, Data Mining, and 803 Report for Fiscal Year 2017. OPTR has reviewed the activities and programs described in this combined report and will continue to work closely with all Treasury bureaus and offices to protect individual privacy and civil liberties in all Treasury activities.

J. Trevor Norris
Acting Assistant Secretary for Management
U.S. Department of the Treasury

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, 2016 through March 31, 2017

Reviews	
Type	Number
Privacy Threshold Analyses (PTAs)/Privacy Impact Assessments (PIAs)	PTA/73 PIA/70
System of Records (SOR) Routine Use/ SOR Notices (SORNs)	1
SSN Elimination or Redaction on Forms	3
Computer Matching Agreements (CMAs)	6
Section 508 Internet Website Scan	79%
Treasury-requested Non-Commerce/Commerce Site Scan	Non-Comm/ 82 Comm/ 89

Advice and Response		
Type	Number	Response
Provide advice and recommendation regarding notice and consent mechanism for system users.	1	Accepted
Provide advice and recommendation regarding the identification of privacy and civil liberties risks and strategies in mitigating these risks.	2	Accepted
Provide advice regarding the publication of PII in publicly available documents.	2	Accepted
Provide advice regarding the disclosure of PIII in accordance with the Privacy Act.	2	Accepted
Provide policy updates to PII Incident Response.	1	Pending

Complaints		
Type	Number	Dispositions
PRIVACY: Claims taxpayer notice mailed to the wrong address.	1	Resolved in favor of Government.
CIVIL LIBERTIES: Claims violation of 4th Amendment Rights.	1	Resolved in favor of Government.
CIVIL IBERTIES: Assertion for violating their 1, 4, and 5th Amendment rights.	8	Pending court date and final decision.