Department of the Treasury

2018 Consolidated Privacy and Civil Liberties Reports

Message from the Assistant Secretary for Management

As the Department of the Treasury's Senior Agency Official for Privacy and Chief Privacy and Civil Liberties Officer, I am pleased to present Treasury's 2018 Consolidated Privacy and Civil Liberties Reports.

- Annual Privacy Report required by Section 522(a) of the Consolidated Appropriations Act of 2005;
- Second semiannual Privacy and Civil Liberties Report required by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007; and
- Annual Data Mining Report requirement in the Federal Agency Data Mining Reporting Act of 2007.

The Department of the Treasury is committed to safeguarding and ensuring privacy compliance through integrated technology, policy and high quality standards. As a collector of data on millions of individuals and companies, the Department strives to be a leader in best privacy practices and privacy policy.

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.

David F. Eisner
Assistant Secretary for Management
U.S. Department of the Treasury

2018 Consolidated Privacy and Civil Liberties 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 second semiannual privacy and civil liberties report required under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007; and

(3) The Data Mining Reporting Act requirement contained in the Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3.

The Reporting Periods

These reports cover Treasury activities during the 2018 fiscal year (FY18). The Annual Privacy and the Data Mining Reporting Act reports cover the entire fiscal year while the Section 803 report covers the second half of FY18 (April 1, 2018 to September 30, 2018); the first Section 803 report for FY18 is a standalone report and can be found on Treasury's Privacy website, https://www.treasury.gov/privacy/annual-reports/Pages/default.aspx.

The Consolidated Appropriations Act of 2005 Annual Privacy Report

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

Section 803 of the 9/11 Commission Act 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 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.

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

Complaints of Privacy Violations

Section 522 of the Consolidated Appropriations Act of 2005 requires Treasury to address in its annual report complaints of privacy violations. Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 ("9/11 Commission Act") requires Treasury to address both privacy and civil liberties complaints. Therefore, both privacy and civil liberties complaints will be addressed in the Section 803 Report in Section 2 of these consolidated reports.

Implementation of the Privacy Act, 5 U.S.C., Section 552a.

System of Records Notices (SORNs)

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]

A complete list of the Department's SORNs is available on Treasury's Privacy Act website, at https://www.treasury.gov/privacy/issuances/Pages/default.aspx

Internal Controls

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. This includes an analysis to ensure compliance with Privacy Act requirements. It allows the assessment of the risks associated with 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. Links to the Treasury's PCLIAs are available on Treasury's website, at https://www.treasury.gov/privacy/PIAs/Pages/default.aspx

[1] *See* 31 C.F.R. §§ 1.20-1.36.

Elimination of the Unnecessary Use of Social Security Numbers

The Social Security Number Fraud Prevention Act of 2017 required Treasury to file an annual report identifying all mailings that include the full Social Security Number (SSN). Over the next four years, Treasury is required to update Congress on its progress in eliminating the mailing of full SSNs. Treasury recently submitted its 2018 report to Congress. For more information on Treasury's usage of SSN, please refer to page 13, Section 6 of this report.

Privacy Policies on Treasury Websites

Treasury maintains online privacy policies to provide notice to Treasury website visitors describing how Treasury collects, uses, shares, and disposes of information it collects on its websites. This includes providing notice about how certain information collected is handled in compliance with the Privacy Act. Treasury bureaus and Treasury's Inspectors General maintain their own online privacy policies to address the unique information they collect on their websites. Links to Treasury bureau and office policies may be found at: https://home.treasury.gov/subfooter/privacy-policy

Treasury Orders and Directives

Treasury Orders (TO) and Treasury Directives (TD) serve as the controls by which Treasury ensures that appropriate stakeholders are involved in privacy and civil liberties policy development and implementation.

Treasury Orders are documents signed by the Secretary or Deputy Secretary that:

- delegate authority from ~~residing in~~ the Secretary or Deputy Secretary to other senior Treasury officials;
- define the organization of the Department and the reporting relationships among the most senior officials; and/or
- establish Treasury policy.

Treasury Orders relevant to this report are:

Treasury Orders	
TO-102-25, Delegation of Authority Concerning Privacy and Civil Liberties	https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to102-25.aspx

Treasury Directives are documents signed by the appropriate senior Treasury officials that:

- ~~may~~ further delegate authority from the most senior officials to other Treasury officials; and/or
- provide processes for implementing legal obligations and Departmental policy objectives.

Treasury Directives relevant to this report are:

Treasury Directives	
TD 25-04, The Privacy Act of 1974, as Amended,	https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td25-04.aspx
TDP, 25-04, The Privacy Act Handbook	https://www.treasury.gov/privacy/Pages/handbook.aspx
TD 25-06, Treasury Data Integrity Board	https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td25-06.aspx
TD 25-07, Privacy Impact Assessments	https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td25-07.aspx
TD 25-08, Safeguarding Against and Responding to the Breach of PII	https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td25-08.aspx
TD 25-09, Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53	https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td25-09.aspx
TD 25-10, Information Sharing Environment Privacy and Civil Liberties Policy	https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td25-10.aspx

Privacy Awareness and Training: A Culture of Privacy Awareness

Subsection (e)(9) of the Privacy Act requires that agencies provide instruction to persons involved in the design, development, operation, or maintenance of systems of records. All Treasury employees are required to take the annual privacy training which includes information regarding the potential criminal penalties and civil liability for employees who do not comply with Privacy Act requirements. In FY18, 98.2% of all Treasury employees successfully completed this training.

Treasury Computer Matching Programs

Pursuant to the Computer Matching and Privacy Protection Act of 1988,[1] Treasury maintains a Data Integrity Board (DIB) to oversee its computer matching programs. Computer matching programs provide a direct benefit to the public by assisting in the elimination of errors and in monitoring waste, fraud, and abuse. 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. For 2018 data on Treasury's Computer matching agreements, please refer to page 13. Treasury computer matching agreements can be found at: https://www.treasury.gov/privacy/Computer-Matching-Programs/Pages/default.aspx

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

SECTION 2: DEPARTMENT OF THE TREASURY SEMIANNUAL 2018 REPORTING ON PRIVACY AND CIVIL LIBERTIES ACTIVITIES PURSUANT TO SECTION 803 OF THE IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007 FOR REPORTING PERIOD APRIL 1, 2018 TO SEPTEMBER 30, 2018

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, TD 25-04, "The Privacy Act of 1974, as amended," designates the Deputy Assistant Secretary for Privacy, Transparency, and Records (DASPTR) as the ASM's principal advisor on issues related to privacy and civil liberties. The DASPTR leads the Office of Privacy, Transparency, and Records (OPTR) and provides the ASM with day-to-day support in executing 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; and
>
> (B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.
>
> (2) Contents –
>
> Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—
>
> a) information on the number and types of reviews undertaken;

b) the type of advice provided and the response given to such advice;
c) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and
d) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

The Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126 (July 7, 2014), changed the reporting period from quarterly to semiannually. The semiannual reports cover the following time periods: April – September and October – March. [2]

2. Privacy and Civil Liberties Reviews Undertaken

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 Assessments are the Treasury mechanism for reviewing IT systems, programs, and other activities to determine whether the program is meeting information compliance requirements (civil liberties, privacy, records management, Section 508 compliance under the Rehabilitation Act of 1973, and Paperwork Reduction Act of 1995,) and to determine whether a more comprehensive Privacy and Civil Liberties Impact Assessment (PCLIA) is required;
b) PCLIAs as required by the E-Government Act of 2002;[3]
c) System of Records Notices, as required by the Privacy Act and any associated Final Rules for Privacy Act exemptions;[4]
d) Privacy Act Statements, as required under the Privacy Act,[4] to provide notice to individuals at the point of collection;
e) Computer Matching Agreements, as required by the Privacy Act;[5]
f) Data Mining Reports, as required by Section 804 of the 9/11 Commission Act of 2007;[6]
g) Privacy Compliance Reviews;
h) Privacy reviews of IT and program budget requests, including Office of Management and Budget Exhibit 300s; and,
i) Other privacy reviews, such as implementation reviews for information sharing agreements.

---

[2] 44 U.S.C. § 3501 note.

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

[4] 5 U.S.C. § 552a(e)(3).

[5] 5 U.S.C. § 552a(o)-(u).

[6] 42 U.S.C. § 2000ee-3.

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 FY18, Treasury published 75 new, updated, or renewed PCLIAs. All published Treasury PCLIAs are available at: http://www.treasury.gov/privacy/PIAs/Pages/default.aspx.

4. System of Records Notices

During the reporting period, Treasury published and updated 1 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 Treasury SORNs.

5. Computer Matching Programs

Treasury participates in 13 active computer matching programs in accordance with the Privacy Act of 1974, as amended. The computer matching provisions of the Privacy Act improve oversight of the disclosure of automated Privacy Act records in inter-agency information sharing arrangements known as matching programs and protect the due process rights of individuals whose records are exchanged in such programs. To comply with the Act, as well as all relevant regulations and guidance, Treasury has established a Data Integrity Board to review and approve associated matching agreements. All Treasury Computer Matching Agreements 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 18-month re-establishment agreements.

6. Privacy Compliance Reviews

Treasury conducts Privacy Compliance Reviews (PCR) to ensure that programs and technologies implement and maintain appropriate protections for PII. A 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. It also includes informal, ad hoc, situational advice sought by Treasury bureaus and offices on privacy and civil liberties issues.

Treasury's major current PCR effort is analyzing departmental mailing of forms, letters, and other documents containing the Social Security Number (SSN). This analysis is required by the SSN Fraud Prevention Act of 2017. 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 continued its review of Treasury's mailing of full SSNs. This exercise is allowing Treasury to update its list of appropriate uses of the SSN and identify SSN uses that can be eliminated. Many Treasury systems remain unable to redact or truncate (shorten) SSNs in outgoing mail due to aging systems and budgetary limitations. During the next reporting period, Treasury will continue its analysis and update its progress in the SSN Fraud Prevention Act.

7. Advice and Responses

Treasury provides privacy advice throughout the year to its bureaus and offices. An example of guidance is 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):*

- Worked with a Treasury program that was contemplating expanding its presence on social media. Notified the program of the privacy and other information management compliance requirements. The program did not go forward with its plans.
- Conducted an assessment of a Treasury program that was undergoing substantial modifications, including the PII it would collect going forward. Advised the program on all Privacy Act and FISMA requirements and assisted with a draft of the PCLIA.
- Continued modifications to the Rules of Behavior for all DO system users to ensure the protection and confidentiality of PII.

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, 2018, through September 30, 2018. 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.

SECTION 3: DEPARTMENT OF THE TREASURY FY2018 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 that is 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. [7]

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 and can be found at https://www.treasury.gov/privacy/annual-reports/Pages/default.aspx .

[7] 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)

FINCEN FY 2018 DATA MINING REPORT

The Federal Agency Data Mining Reporting Act of 2007 requires the head of each Department or agency of the Federal Government that is engaged in any activity that uses or develops data mining to submit a report to Congress on all pattern-based data mining activities. Each report must include the following information for each activity where data mining is in use or in development:

(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.

The mission of the Financial Crimes Enforcement Network (FinCEN) is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence. 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 and 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, Public Law 107-56, October 26, 2001 and to implement and administer the provisions of the Bank Secrecy Act (BSA).

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 multiple types of illicit financial activity, including money laundering, terrorist financing, and cybercrime. 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 generate 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 Bank Secrecy Act (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 as domestic law enforcement and foreign 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. The 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 use FinCEN's "Advanced Analytics" system. This system is comprised of commercial off-the-shelf 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 collected 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 Fin CEN 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 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

[8] 31 U.S.C. § 5318(g).

[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 information, please visit the NTIS website.

consumers has different restrictions or guidelines under which FinCEN can provide BSA data or BSA data derived analysis.

In FY 2018, FinCEN produced a total of 1,983 financial intelligence products for law enforcement partners and, in addition to these products, FinCEN also responded to 409 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 Group[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 terrorist financing, money laundering, and fraud against the U.S. government to include healthcare fraud and income tax fraud.

- To combat terrorist financing threats, FinCEN has developed more than 25 business rules designed to identify and disrupt terrorist organizations' revenue streams and target their financial support networks. The rules generate more than 3,800 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 3,700 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.

- 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, found in the BSA information submitted to FinCEN that identifies those 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

[10] The Egmont Group is a united body of 157 FIUs. The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing

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 on FinCEN's website. Readers accessed the interactive SAR Stats module an average of 49,000 times per month with approximately 1,600 daily users in fiscal year 2018. Since going live in March 2015, interactive SAR Stats has received more than 1.6 million 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 of individuals has been and will continue to be minimal. As a threshold matter, the Supreme Court has ruled that 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), carries no constitutionally protected "expectation of privacy."[11] Moreover, the Right to Financial Privacy Act of 1978[12] expressly provides that it gives 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.[13] 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,[14] 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

[11] *United States v. Miller*, 425 U.S. 435, 442 (1976).

[12] 12 U.S.C. § 3401, *et seq.*

[13] 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.")

[14] 5 U.S.C. § 552a.

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 Privacy Impact Assessments (PIA) on its public website, which informs the public of FinCEN's activities and practices related to the collection, processing, retention, and distribution of personally identifiable information (PII).[15]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.

(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."

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.

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

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."[16] 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."[17] 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:

(1) Treasury/FinCEN .001, *FinCEN Investigations and Examinations System*;[18]

[16] 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 assigned to the individual);

[17] 5 U.S.C. § 552a(b)(3).

[18] 79 Fed. Reg. 20969 (April 14, 2014).

(2) Treasury/FinCEN .002, *Suspicious Activity Report (SAR) System*; [19] and

(3) Treasury/FinCEN .003, *Bank Secrecy Act (BSA) Reports System*.[20]

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.[21] 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.[22]

FinCEN is required to "analyze and disseminate" the data for a broad range of purposes consistent with the law.[23] 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

---

[19] *Id*. at 20972.

[20] *Id*. at 20974.

[21] 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).

[22] 31 U.S.C.§ 310(b)(2)(B).

[23] *Id*. at § 310(b)(2)(C)(i)-(vii).

[24] *Id.* at § 310(b)(2)(E), (G).

[25] *Id*. at § 310(c)(1) and (c)(2).

tracking and controlling foreign assets."[24] The section also provides for the establishment of standards for making the information available through efficient means, and to screen appropriate users and appropriate uses.[25] 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.

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 and FinCEN 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 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.

ALCOHOL AND TOBACCO TAX AND TRADE BUREAU (TTB) FY 2018 DATA MINING REPORT

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 performs two types[26] 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; and
- Searches of commercial and law enforcement databases to discover criminal activity.

TTB conducts these activities primarily for the purpose of compiling business intelligence reports that identify 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 is gathered through queries of registered individuals or businesses, and include some queries that are solely based on subject matter (for example, queries of all tobacco product imports over a given time period).

The goals of TTB's analytics program are to provide business intelligence to improve detection of common violations and to automate certain routine oversight processes. These activities may identify compliance risks and potential criminal activity that may be flagged for further field review and action.

(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 TTB field staff determines whether a particular pattern or anomaly is indicative of violations that may be subject to further field review and investigation.

Most data mining is conducted with a combination of SAS statistical analysis software 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 is collected and transformed, TTB develops reports that consolidates specific factors along with business rules that flag entities needing additional research. This additional research may serve as the basis of referral for further TTB action.

[26] In prior TTB conducted some link analysis between businesses, individuals and associates however did not conduct this activity in FY 18.

(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; and
- Certification/Exemption of Label/Bottle Approvals (COLAS) Online–data from businesses 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;
- Financial Crimes Enforcement Network Query (FinCEN Query) – data submitted in compliance with the Bank Secrecy Act transcripts such as Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), etc.; and
- LexisNexis Accurint – public records data of court proceedings (including some criminal cases), property holdings, licenses, and registrations. This is a for fee 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 automates certain routine screening and monitoring processes to improve identification of criminal activity and detection of compliance violations. Business intelligence reports automatically consolidate data and monitor patterns in operations, tax payments, and import and export activity. This automation and business intelligence enables TTB to provide oversight to a wider selection of its regulated industries. For FY18, there was a 65% success rate for initiation of cases through the use of analytics.

(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 vigorously protected against unauthorized use and disclosure. 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 this 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 with FinCEN, dated May 3, 2005, TTB is granted 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 granted for tax or regulatory purposes relevant to the mission of TTB.

The authority to collect excise taxes on imported alcohol and tobacco products was originally retained by the Secretary of the Treasury 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)).

TTB is authorized pursuant to the Homeland Security Act of 2002, Pub. L. 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) to access data within Customs and Border Protection (CBP) data systems necessary to fulfill its 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 reports consists of taxpayer information, 26 U.S.C. § 6103 governs the use of all tax-related data. 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 the 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 at 80 F.R. 4637 (January 28, 2015).

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 business intelligence receive training in the proper handling of information. Users receive demonstrations of the reports and have access to a user guide. 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. For all available governmental data sources, users must sign a non-disclosure agreement before receiving access.

(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 models to take any adverse action against any individual or entity. Rather, the reports 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.

INTERNAL REVENUE SERVICE (IRS) FY 2018 DATA MINING REPORT

(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 organization (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 2018, each of these IRS divisions used one or more 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);
- Return Review Program (RRP);
- FinCEN Query; and
- Compliance Data Warehouse (CDW)

IRS-CI is tasked with protecting IRS revenue streams by detecting fraudulent activity and preventing recurrences. In FY 2018, IRS-CI used IDEA, LCA, 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 with 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 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 LCA 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 LCA application enable users to detect suspicious financial transactions indicative of money laundering, terrorism, and other financial crimes. 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. It also 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 Bank Secrecy Act (BSA) Suspicious Activity Report (SAR) reviews and Financial Crimes Task Force activity.

IRS-CI and W&I use RRP to maximize detection of tax return fraud, tax noncompliance, and identity theft. As RRP receives returns, it loads and assigns a risk score to each tax return based on an array of models. Scores range from 0.0 to 1.0, with a higher score indicating a greater potential for fraud. In addition to models, RRP also includes multiple model scores and linking characteristics. In RRP, 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. RRP employs multiple technologies for data mining activities. Each of these technologies use current year examples of identity theft (IDT), non-IDT tax fraud, and non-fraud to develop supervised models, unsupervised models, rules, and network analytics

IRS-CI and SB/SE users access the FinCEN Query system (see FinCEN report herein) as the system of record for Bank Secrecy Act (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 and better sharing of data assets. A large and diverse set of use patterns includes:

- Machine learning. Used to detect ID theft and refund fraud patterns; develop return-based scores for compliance planning; identify anomalies for case selection; embed case routing and treatment strategies into collection processes; and predict issue categorization in customer service workstreams.
- Natural language processing. Used to better understand behavioral factors in taxpayer decisions; categorize appeals determinations; identify related entities, material advisors, and other parties in complex business structures; compare third-party documents; and analyze topics and sentiment in voice recordings. Also used for language translation to convert machine-readable text from dozens of foreign languages to English to facilitate other analytical methods.
- Graph-based analytics. Used to identify complex relationships in corporate flow-throughs, tax shelters, entity fabrication, and pyramiding schemes; detect anomalies in preparer networks; develop risk-based models for multi-party transactions; and model the diffusion of tax law changes through internal orders, process controls, and policies.
- Simulation. Used to perform what-if calculations for changes in tax policy; develop models of taxpayer choice for customer service channels; model tax evasion for pass-through entities; and estimate taxpayer burden measures.
- Optimization. Used to create dynamic, next-best-case recommendation for workload delivery; develop enterprise staffing attrition models; and identify optimal post-of-duty locations.

(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 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[27] 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 RRP from the Generalized Mainline Framework (GMF).[28] This allows W&I and SDC employees to review those returns for suspicious activities.

If a return met designated score tolerances and other criteria, W&I and IRS-CI personnel examined 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 Electronic Fraud Detection System Case Management 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 use current 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 run 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 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.

[27] QRP was referenced in last year's report as a subsystem of EFDS Data Mining. EFDS-DM was removed from the report because IRS's fraud detection and revenue protection functions was migrated from EFDS to the RRP. RRP is using GMF feeds for its source. As a result, the QRP reference is no longer applicable.

[28] 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.

a) RRP's network analytics tool – Linked Return Analysis (LRA) – uses multiple custom built Greenplum functions to link returns that display common, suspicious characteristics.
b) 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 Blaze Advisor. 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. Analytical tools include SAS, Stata, R, Python, Neo4j, Hadoop, Spark, Apache Zeppelin, Tableau, ArcGIS, ExtendSim, NetLogo, Repast HPC, Cytoscape, Solr, ElasticSearch, Tesseract, Tensorflow, and BigSQL for machine learning, graph-based analytics, natural language processing, simulation, optimization, and advanced visualization. Database technology includes SAP IQ, SAP Hana, SAP Data Services, Oracle, SQL Server, PostgreSQL, and MongoDB. International Mathematics and Statistics Libraries are used to create user-defined functions for in-database analytics. CDW provides a self-service model that allows users to dynamically explore and test data-driven business problems. It is a general-purpose analytical computing environment, not an application.

(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 Modernized e-File (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 RRP application leverages the following data sources.

- **Taxpayer**: The source is the electronically filed return (as transmitted through MeF) or a paper filed tax return. RRP also loads 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**: All states and the District of Columbia prisons 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 MeF or as a paper filed tax return
- **Employers/Payers:** Information from employers/payers captured on various forms as stored in the 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 under reporter 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 is no empirical data on the efficacy of searches by the IDEA and LCA applications.

The efficacy of RRP can be measured in terms of identity theft detection and ability to identify returns ready for non-identity theft compliance referral treatment. Two key metrics are used to assess RRP's efficacy: lead generation and True Positive Rate. In FY 2018 (through December 31, 2018), RRP generated over 1,125,000 identity theft leads at a lead accuracy rate of 48 percent. This represents a 32 percent increase in ID theft leads produced by RRP versus the same period in FY 2017. Almost 5 out of every 10 returns flagged as IDT by RRP never receive a legitimate taxpayer identity authentication via the IRS' web, phone, or in-person authentication processes.

In addition to identity theft detections, RRP includes models to identify returns ready for non-identity theft compliance referral treatment. RRP expanded its capability in this area in 2018 by adding models that target returns claiming the Earned Income Tax Credit (EITC) or the Additional Child Tax Credit (ACTC) to leverage the capabilities provided by Congress in the Protecting Americans Against Tax Hikes (PATH) Act of 2015. During 2018, RRP increased the non-identity theft fraud leads by over 500 percent versus the same period in FY 2017 - an increase in over 1,000,000 new non-identity theft fraud leads:

- RRP Non-Identity Theft Models/Filters: over 485,000 leads at 38 percent lead accuracy
- EIC/ACTC Models/Filters (new for FY 2018): over 580,000 leads at 18 percent accuracy
- RRP Business Rules Filters: over 60,000 leads at 4 percent lead accuracy
- RRP Frivolous Filer Rules: over 199,000 leads at 2 percent lead accuracy

The efficacy of the FinCEN Query system is discussed herein 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 or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of implementing the data mining activity.

Once evidence of fraud is discovered, laws and administrative procedures, policies, and controls govern the ensuing actions. IDEA, LCA, and CDW applications use personally identifiable information (PII) for pattern matching but the results of a query or analysis are used for further investigation. IRS CI and RAAS follow the IRS security and privacy IRM standards and regulations for the use and protection of PII.

The impact or likely impact of 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. IRS has a system, Online 5081, that governs program access authorization.

RRP data mining activities, including machine learning and scoring processes, do not directly use PII in determining whether a return is likely to be fraudulent. Scoring occurs on the characteristics of the return in question, not on 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 collected, reviewed, gathered, analyzed, or used in 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 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.

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 resulting from queries or statistical analysis in IDEA, LCA, and CDW are used as a lead or as insights for actionable decisions 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 IDEA, LCA, and CDW systems.

RRP does not determine 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, 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.

IDEA, LCA, and CDW are not the authoritative owners of data. However, data is used for investigative or research purposes under the IRS Internal Revenue Manual (IRM) standards and guidelines. The data resulting from query searches is used as a lead or as insights for actionable decisions and requires additional investigative steps to verify the quality of the information. CI and RAAS use this data for generating leads and other data-driven insights that are subsequently verified by special agents or research analysts for further investigative or analytical work.

CDW implements a standard set of rules during the extract, transformation, and load (ETL) process to ensure that data collected from authoritative systems is accurately replicated for research purposes. These include, but are not limited to, 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 RRP used for data mining are based on outside data sources. The only data generated in RRP is 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 RRP matches the data from the input source and that the system accurately displays the data in the 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.

Combined Reports Conclusion

The Department of the Treasury is pleased to provide to Congress its Annual Privacy, Section 803 Report, and Data Mining Report, for Fiscal Year 2018. 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.

David F. Eisner
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 April 1, 2018 through September 31, 2018

Reviews		Advice and Response			Complaints		
Type	**Number**	**Type**	**Number**	**Response (Pending/ Accepted/in Process)**	**Type of claim or assertion in complaint**	**# of complaints**	**Disposition**
Privacy (and Civil Liberties) Threshold Analyses (PTAs/PCLTAs)	51	Provide advice and recommendation regarding proper handling of PII/limiting access based on need to know	104	Accepted	PRIVACY: Unauthorized disclosure (internal/ external)	Internal: 3 External: 2	Internal: 1 employee counseled; 1 employee reprimanded; case closed after confirmation no PII disclosure. External: Offered identity theft protection.
Privacy (and Civil Liberties) Impact Assessments (PIAs/PCLIAs)	75	Provide advice and/or recommendation on relevance and necessity of data collection/ingestion	25	Accepted	PRIVACY: Complaint regarding SSN on IRS notice	External: 1	Responded with explanation of legal requirement
System of Records (SOR) Routine Use/ SOR Notices (SORNs)	1	Provided guidance to system owners or personnel on necessary privacy compliance documentation or appropriate NIST risk rating.	77	Accepted	PRIVACY: Improper handling of PII documents	1	Investigation ongoing
Computer Matching Agreements (CMAs)	13	Provide advice and recommendation on internal/external sharing of PII (including Privacy Act info)	64	Accepted	CIVIL LIBERTIES: Violation 1st, 4th, 5th, 6th, 14th and/or 16th Amendment rights	11 (# of complaints/amendments alleged to have been violated)	4 - Pending court date and final decision 7 - Resolved in favor of Government
		Provide advice and recommendation on web privacy policies/privacy notices	13	Accepted	CIVIL LIBERTIES: (Other: Describe)		