**BILLING CODE 4810-25-P**

**DEPARTMENT OF THE TREASURY**

Departmental Offices

**Privacy Act of 1974; Systems of Records**

**AGENCY:** Departmental Offices, Treasury.

**ACTION:** Notice of systems of records.

**SUMMARY:** In accordance with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a, the Departmental Offices (DO) is publishing its Privacy Act systems of records.

**SUPPLEMENTARY INFORMATION:** Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a and the Office of Management and Budget (OMB) Circular No. A-130, the Department completed a review of its Privacy Act systems of records notices to identify and implement minor changes that more accurately describe these records. Such changes throughout the document are editorial and consist principally of changes to system locations and system manager addresses, and revisions to organizational titles. The notices were last published in their entirety on January 2, 2014, beginning at 79 FR 209.

Two systems of record have been amended, altered, or added to the Department's inventory of Privacy Act notices since January 2, 2014, as follows:

DO .016 - Multiemployer Pension Reform Act of 2014 (MPRA)" (March 16, 2016 at 81 FR 14223) Treasury uses the system to account for all individuals eligible to vote in elections with respect to benefit suspensions under MPRA whose information is furnished by the plan sponsors proposing the benefit suspensions and DO .411 Intelligence Enterprise Files (September 26, 2014 at 79 FR 58042) The records are used to fulfill OIA's statutory and Executive Order mandates to collect (overtly or through publicly-available sources), receive, analyze, collate,

produce, and disseminate information, intelligence, and counterintelligence related to the operations and responsibilities of the entire Department, including all components and bureaus.

In addition, as a part of this Biennial review, the Department is updating and reissuing two systems of records, including: DO .144 -General Counsel Litigation Referral and Reporting System and DO .214 -DC Pensions Retirement Records. These updates are discussed below:

(1) DO .144 - General Counsel Litigation Referral and Reporting System, which now includes an expanded purpose, to "keep track of component assigned to handle a particular litigation action." DO.144 also includes an update to routine use (1) to "Disclose information to the Department of Justice (DOJ) (including United States Attorneys' Offices) or other federal agencies conducting litigation or in proceedings before any court or adjudicative or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: a. Treasury or any component thereof; b. Any employee of Treasury in his/her official capacity; c. Any employee of Treasury in his/her individual capacity where the Department of Justice or Treasury has agreed to represent the employee; or, The United States or any agency thereof."

This routine use seeks to specify that the Department routinely discloses litigation information to DOJ under the above limited circumstances. The Department previously relied on more general routine use language to discuss disclosure to other federal agencies. However, this change more accurately discusses the routine disclosure to DOJ. The Department has reviewed this routine use and determined that it is compatible with the purpose of collecting the records. The system collects information for the purpose of responding to inquiries from the DOJ and other agencies, therefore the routine disclosure to DOJ is in accordance with the purpose of collection.

(2) DO .214-DC Pensions Retirement Records, now includes changes to three routine uses discussed below: Routine use (4) now states "To disclose information to another federal agency, to a court, or to a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the federal government is a party to the judicial or administrative proceeding. In those cases where the federal government is not a party to the proceeding, records may not be disclosed unless the party complies with the requirements of 31 C.F.R. 1.11." This routine use has been slightly altered to include the exceptions to non-disclosure when the government is not a party to a proceeding, cited in 31 C.F.R. 1.11. The routine use refers to 31 C.F.R. 1.11, which sets forth the policies and procedures of the Department regarding the production or disclosure of information contained in Department documents for use in legal proceedings pursuant to a request, order, or subpoena (collectively referred to in this subpart as a demand).

Routine use (6) has been altered to include clarifying language and now includes the following language: "To disclose information to the Department of Justice when seeking legal advice, or for use in any proceeding, or to prepare for a proceeding, when any of the following is a party to, has an interest in, or is likely to be affected by the proceeding: (A) The Department or any component thereof; (B) Any employee of the Department in his or her official capacity; (C) Any employee of the Department in his or her individual capacity where the Department of Justice or the Department has agreed to represent the employee; or (D) The federal funds established by the Act to pay benefit payments. This routine use more specifically discusses the circumstances under which the Department will disclose D.C. Pension information to the DOJ.

DO.214 also includes a new routine use (11) which includes the following language, "To disclose health insurance enrollment information to OPM. OPM provides this enrollment

information to their health care carriers who provide a health benefits plan under the Federal Employees Health Benefits Program, or health insurance carriers contracting with the District to provide a health benefits plan under the health benefits program for District employees, Social Security numbers and other information necessary to identify enrollment in a plan, to verify eligibility for payment of a claim for health benefits, or to carry out the coordination for benefits provisions of such contracts."

The Department has reviewed these routine uses and determined that they are compatible with the purpose of collecting the records. Each routine use listed above is compatible with the original purpose of collection, specifically, to provide information on which to base determinations of (1) eligibility for, and computation of, benefit payments and refund of contribution payments; (2) direct deposit elections into a financial institution; (3) eligibility and premiums for health insurance and group life insurance; (4) withholding of income taxes; (5) under- or over-payments to recipients of a benefit payment, and for overpayments, the recipient's ability to repay the overpayment; (6) Federal payment made from the General Fund to the District of Columbia Pension Fund and the District of Columbia Judicial Retirement and Survivors Annuity Fund; (7) impact to the Funds due to proposed Federal and/or District legislative changes; and (8) District or Federal liability for benefit payments to former District police officers, firefighters, and teachers, including survivors, dependents, and beneficiaries who are receiving a Federal and/or District benefit.

**Systems Covered by This Notice**

This notice covers all systems of records maintained by the Departmental Offices as of [enter date of FR publication]. The system notices are reprinted in their entirety following the Table of Contents.

_____

Ryan Law,

Acting Deputy Assistant Secretary for Privacy, Transparency, and Records

**Departmental Offices (DO)**

**Table of Contents**

DO .003--Law Enforcement Retirement Claims Records

DO .007--General Correspondence Files

DO .010--Office of Domestic Finance, Actuarial Valuation System

DO .015--Political Appointee Files

DO .016--Multiemployer Pension Reform Act of 2014 (MPRA)

DO .060--Correspondence Files and Records on Dissatisfaction

DO .120--Records Related to Office of Foreign Assets Control Economic Sanctions

DO .144--General Counsel Litigation Referral and Reporting System

DO .149--Foreign Assets Control Legal Files

DO .190--Office of Inspector General Investigations Management

Information System (formerly: Investigation Data Management System)

DO .191--Human Resources and Administrative Records System

DO .193--Employee Locator and Automated Directory System

DO .194--Circulation System

DO .196--Treasury Information Security Program

DO .202--Drug-Free Workplace Program Records

DO .207--Waco Administrative Review Group Investigation

DO .209--Personal Services Contracts (PSC)

DO .214--DC Pensions Retirement Records

DO .216--Treasury Security Access Control and Certificates Systems

DO .217--National Financial Literacy Challenge Records

DO .218--Making Home Affordable Program

DO .219--TARP Standards for Compensation and Corporate Governance--

Executive Compensation Information

DO .220--SIGTARP Hotline Database

DO .221--SIGTARP Correspondence Database

DO .222--SIGTARP Investigative MIS Database

DO .223--SIGTARP Investigative Files Database

DO .224--SIGTARP Audit Files Database

DO .225--TARP Fraud Investigation Information System

DO .226--Validating EITC Eligibility with State Data Pilot Project Records

DO .301--TIGTA General Personnel and Payroll

DO .302--TIGTA Medical Records

DO .303--TIGTA General Correspondence

DO .304--TIGTA General Training

DO .305--TIGTA Personal Property Management Records

DO .306--TIGTA Recruiting and Placement Records

DO .307--TIGTA Employee Relations Matters, Appeals, Grievances, and Complaint Files

DO .308--TIGTA Data Extracts

DO .309--TIGTA Chief Counsel Case Files

DO .310--TIGTA Chief Counsel Disclosure Section

DO .311--TIGTA Office of Investigations Files

DO .411--Intelligence Enterprise Files.

**TREASURY/DO .003**

**System name:**

Law Enforcement Retirement Claims Records--Treasury/DO.

**System location:**

These records are located in the Office of Human Capital Strategic Management, Suite 1200, 1750 Pennsylvania Avenue, NW, Department of the Treasury, Washington, DC 20220.

**Categories of individuals covered by the system:**

Current or former Federal employees who have submitted claims for law enforcement retirement coverage (claims) with their bureaus in accordance with 5 U.S.C. 8336(c)(1) and 5 U.S.C. 8412(d).

**Categories of records in the system:**

The system contains records relating to claims filed by current and former Treasury employees under 5 U.S.C. 8336(c)(1) and 5 U.S.C. 8412(d). These case files contain all documents related to the claim including statements of witnesses, reports of interviews and hearings, examiner's findings and recommendations, a copy of the original and final decision, and related correspondence and exhibits.

**Authority for maintenance of the system:**

5 U.S.C. 8336(c)(1), 8412(d), 1302, 3301, and 3302; E.O. 10577; 3 CFR 1954-1958 Comp., p. 218 and 1959-1963 Comp., p. 519; and E.O. 10987.

**Purpose(s):**

The purpose of the system is to make determinations concerning requests by Treasury employees that the position he or she holds qualifies as a law enforcement position for the purpose of administering employment and retirement benefits.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used:

(1) To disclose pertinent information to the appropriate federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(2) To disclose information to any source from which additional information is requested in the course of processing a claim, to the extent necessary to identify the individual whose claim is being adjudicated, inform the source of the purpose(s) of the request, and identify the type of information requested;

(3) To disclose information to a federal agency, in response to its request, in connection with the hiring or retention of an individual, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the

extent that the information is relevant and necessary to requesting the agency's decision on the matter;

(4) To provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(5) To disclose information which is relevant and necessary to the Department of Justice or to a court when the Government is party to a judicial proceeding before the court;

(6) To provide information to the National Archives and Records Administration for use in records management inspections conducted under authority of 44 U.S.C. 2904 and 2908;

(7) To disclose information to officials of the Merit Systems Protection Board, the Office of the Special Counsel, the Federal Labor Relations Authority, the Equal Employment Opportunity Commission, or the Office of Personnel Management when requested in performance of their authorized duties;

(8) To disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing Counsel or witnesses in the course of civil discovery, litigation or settlement negotiations in response to a court order where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings; and

(9) To provide information to officials of labor organizations recognized under the Civil Service Reform Act when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting work conditions.

(10) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or

harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by names of the individuals on whom they are maintained.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

In accordance with General Records Schedule 1, Civilian Personnel Records, Category 7d are disposed of after closing of the case.

**System manager(s) and addresses:**

Director, Office of Human Capital Strategic Management, Suite 1200, 1750 Pennsylvania Avenue, NW, Department of the Treasury, Washington, DC 20220.

**Notification procedure:**

It is required that individuals submitting claims be provided a copy of the record under the claims process. They may, however, contact the agency personnel or designated office where the action was processed, regarding the existence of such records on them. They must furnish the following information for their records to be located and identified: (1) name, (2) date of birth, (3) approximate date of closing of the case and kind of action taken, (4) organizational component involved.

**Record access procedures:**

It is required that individuals submitting claims be provided a copy of the record under the claims process. However, after the action has been closed, an individual may request access to the official copy of the claim file by contacting the system manager. Individuals must provide the following information for their records to be located and identified: (1) name, (2) date of birth, (3) approximate date of closing of the case and kind of action taken, (4) organizational component involved.

**Contesting record procedures:**

Review of requests from individuals seeking amendment of their records which have been the subject of a judicial or quasi-judicial action will be limited in scope. Review of amendment requests of these records will be restricted to determining if the record accurately documents the action of the agency ruling on the case, and will not include a review of the merits of the action, determination, or finding. Individuals wishing to request amendment to their

records to correct factual errors should contact the system manager. Individuals must furnish the following information for their records to be located and identified: (1) name, (2) date of birth, (3) approximate date of closing of the case and kind of action taken, (4) organizational component involved.

**Record source categories:**

Information in this system of records is provided: (1) by the individual on whom the record is maintained, (2) by testimony of witnesses, (3) by agency officials, (4) from related correspondence from organizations or persons.

**Exemptions claimed for the system:**

None.

**TREASURY/DO.007**

**System name:**

General Correspondence Files--Treasury/DO.

**System location:**

Departmental Offices, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220. Components of this record system are in the following offices within the Departmental Offices:

1. Office of Foreign Assets Control.
2. Office of Tax Policy.
3. Office of International Affairs.
4. Office of the Executive Secretariat.
5. Office of Legislative Affairs.
6. Office of Terrorism and Financial Intelligence.

**Categories of individuals covered by the system:**

Members of Congress, U.S. Foreign Service officials, officials and employees of the Treasury Department, officials of municipalities and State governments, and the general public, foreign nationals, members of the news media, businesses, officials and employees of other Federal Departments and agencies.

**Categories of records in the system:**

Incoming correspondence and replies pertaining to the mission, function, and operation of the Department, tasking sheets, and internal Treasury memorandum.

Authority for maintenance of the system:

5 U.S.C. 301.

**Purpose(s):**

The manual systems and/or electronic databases (e.g., Treasury Automated Document System (TADS)) used by the system managers are used to manage the high volume of correspondence received by the Departmental Offices and to accurately respond to inquiries, suggestions, views and concerns expressed by the writers of the correspondence. It also provides the Secretary of the Treasury with sentiments and statistics on various topics and issues of interest to the Department.

**Routine uses of records maintained in the system including categories of users and the purposes of such uses:**

These records may be used to:

(1) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(2) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2 which relate to an agency's functions relating to civil and criminal proceedings;

(3) Provide information to unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114;

(4) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(5) Provide information to appropriate federal, state, local, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license;

(6) Provide information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings, and

(7) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name of individual or letter number, address, assignment control number, or organizational relationship.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

Some records are maintained for three years, then destroyed by burning. Other records are updated periodically and maintained as long as needed. Some electronic records are periodically updated and maintained for two years after date of response; hard copies of those records are disposed of after three months in accordance with the NARA schedule. Paper records of the Office of the Executive Secretary are stored indefinitely at the Federal Records Center.

**System manager(s) and addresses:**

1. Director, Office of Foreign Assets Control, U.S. Treasury Department, Room 2233, Treasury Annex, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

2. Freedom of Information Act Officer, Office of Tax Policy, U.S. Treasury Department, Room 5037G-MT, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

3. Senior Director, International Affairs Business Office, U.S. Treasury Department, Room 4456-MT, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

4. Director, VIP Correspondence, Office of the Executive Secretariat, U.S. Treasury Department, Room 3419-MT, Washington, DC 20220.

5. Deputy to the Assistant Secretary, Office of Legislative Affairs, U.S. Treasury Department, Room 3464-MT, Washington, DC 20220.

6. Senior Resource Manager, Office of Terrorism and Financial Intelligence, U.S. Department of the Treasury, Room 4006, Washington, DC 20220.

**Notification Procedure:**

Individuals wishing to be notified if they are named in this system of records, or to gain access to records maintained in this system may inquire in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Individuals must submit a written request containing the following elements: (1) identify the record system; (2) identify the category and type of records sought; and (3) provide at least two items of secondary identification (date of birth, employee identification number, dates of employment, or similar information). Address inquiries to Director, Disclosure Services (see ``Record access procedures'' below).

**Record Access procedures:**

Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting Record procedures:**

See "Record access procedures" above.

**Record source categories:**

Members of Congress or other individuals who have corresponded with the Departmental Offices, other governmental agencies (federal, state, and local), foreign individuals and official sources.

**Exemptions claimed for the system:**

None.

**TREASURY/DO.010**

**System name:**

Office of Domestic Finance, Actuarial Valuation System--Treasury/DO.

**System location:**

Departmental Offices, Office of Government Financing, Office of Policy and Legislative Review, 1120 Vermont Avenue, NW, Washington, DC 20005.

**Categories of individuals covered by the system:**

Participants and beneficiaries of the Foreign Service Retirement and Disability System and the Foreign Service Pension System. Covered employees are located in the following agencies: Department of State, Department of Agriculture, Agency for International Development, Peace Corps, and the Department of Commerce.

**Categories of records in the system:**

Active Records: name; social security number; salary; category-grade; pay-plan; department-class; year of entry into system; service computation date; year of birth; year of resignation or year of death, and refund if any.

Retired Records: same as active records; annuity; year of separation; cause of separation (optional, disability, deferred, etc.); years and months of service by type of service; marital status; spouse's year of birth; annuitant type; principal's year of death; number of children on annuity roll; children's years of birth and annuities.

**Authority for maintenance of the system:**

22 U.S.C. 4058 and 22 U.S.C. 4071h.

**Purpose(s):**

22 U.S.C. 4058 and 22 U.S.C. 4071h require that the Secretary of the Treasury prepare estimates of the annual appropriations required to be made to the Foreign Service Retirement and Disability Fund. The Secretary of the Treasury is also required, at least every five years, to prepare valuations of the Foreign Pension System and the Foreign Service Retirement and Disability System. In order to satisfy this requirement, participant data must be collected so that liabilities for the Foreign Service Retirement and Disability System and the Foreign Service Pension System can be actuarially determined.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

(1) Data regarding specific individuals is released only to the contributing agency for purposes of verification, and

(2) Other information may be disclosed to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved alphabetically.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a

need to know the information for the performance of their official duties and who have appropriate clearances or permissions. Access is restricted to select employees of the Office of Government Financial Policy. Passwords are required to access the data.

**Retention and disposal:**

Records are retained on a multiple year basis in order to perform actuarial experience studies.

**System manager(s) and address:**

Director, Office of Policy and Legislative Review, Departmental Offices, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, gain access to records maintained in this system, or seek to contest its content must submit a written request containing the following elements: (1) identify the record system; (2) identify the category and type of records sought; and (3) provide at least two items of secondary identification (date of birth, employee identification number, dates of employment, or similar information). Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Record Access procedures:**

See "notification procedure" above.

**Contesting Record procedures:**

See "notification procedure" above.

**Record source categories:**

Data for actuarial valuation are provided by organizations responsible for pension funds and pay records, namely the Department of State and the National Finance Center.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .015**

**System name:**

Political Appointee Files--Treasury/DO.

**System location:**

Department of the Treasury, Departmental Offices, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Individuals who may possibly be appointed to political positions in the Department of the Treasury, consisting of Presidential appointees requiring Senate confirmation; non-career Senior Executive Service appointees; and Schedule C appointees.

**Categories of records in the system:**

Files may consist of the following: Referral letters; White House clearance letters; information about an individual's professional licenses (if applicable); IRS results of inquiries; notation of National Agency Check (NAC) results (favorable or otherwise); internal memoranda concerning an individual; Financial Disclosure Statements (Standard Form 278); results of inquiries about the individual; Questionnaire for National Security Positions Standard Form 86; Personal Data Statement and General Counsel Interview sheets; published works including books, newspaper and magazine articles, and treatises by the individual; newspaper and

magazine articles written about or referring to the individual; and or articles containing quotes by the individual, and other correspondence relating to the selection and appointment of political appointees.

**Authority for maintenance of the system:**

5 U.S.C. 3301, 3302 and E.O. 10577.

**Purpose(s):**

These records are used by authorized personnel within the Department to determine a potential candidate's suitability for appointment to non-career positions within the Department of the Treasury.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be disclosed to:

(1) The Office of Personnel Management, Merit Systems Protection Board, Equal Employment Opportunity Commission, and General Accounting Office for the purpose of properly administering Federal personnel systems or other agencies' systems in accordance with applicable laws, Executive Orders, and regulations;

(2) A federal, state, local, or foreign agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information that has requested information relevant to or necessary to the requesting agency's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) A court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation or

settlement negotiations in response to a court order where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(4) A congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(5) Third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(6) Appropriate federal, state, local, or foreign agencies responsible for investigating or prosecuting the violation of, or for implementing a statute, regulation, order, or license, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation, and

(7) To appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are store on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by last name of individual and Social Security Number.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearance or permissions. Building employs security guards.

**Retention and disposal:**

Records are destroyed at the end of the Presidential administration during which the individual is hired. For non-selectees, records of individuals who are not hired are destroyed one year after the file is closed, but not later than the end of the Presidential administration during which the individual is considered.

**System manager(s) and address:**

White House Liaison, Department of the Treasury, Room 3418, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be informed if they are named in this system or gain access to records maintained in the system must submit a written, signed request containing the following elements: (1) identify the record system; (2) identify the category and type of records sought; and (3) provide at least two items of secondary identification (date of birth, employee identification number, dates of employment, or similar information). Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Record access procedures:**

See "Record Notification procedure" above.

**Contesting record procedures:**

See "Record Notification procedure" above.

**Record source categories:**

Records are submitted by the individuals and compiled from interviews with those individuals seeking non-career positions. Additional sources may include the White House, Office of Personnel Management, Internal Revenue Service, Department of Justice and international, state, and local jurisdiction law enforcement components for clearance documents, and other correspondence and public record sources.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .016**

## System name:

Multiemployer Pension Reform Act of 2014

## System location:

System records are located at one or more service providers under contract with the Department of the Treasury, Departmental Offices, 1500 Pennsylvania Ave. NW, Washington, DC 20220

## Categories of individuals covered by the systems:

Individuals identified as participants or beneficiaries of deceased participants by plan sponsors that have submitted an application for suspension of benefits under the Multiemployer Pension Reform Act of 2014.

## Categories of records in the systems:

Personal contact information, including, but not limited to:

- Mailing addresses;
- Phone numbers;
- Electronic mail (Email) addresses; and
- Information sufficient to tabulate electronic votes and check the integrity of voting systems.

## Authority for maintenance of the systems:

Multiemployer Pension Reform Act of 2014, Division O of the Consolidated and Further Continuing Appropriations Act 2015, Pub. L. No. 113-235.

## Purposes:

The system is maintained to support the provision of ballot packages to individuals identified as participants or beneficiaries of deceased participants by plan sponsors that have submitted an application for suspension of benefits under the Multiemployer Pension Reform Act of 2014, and may be used to provide technical support to voters in connection with the ballots and to check the integrity of the election.

## Routine uses of records maintained in the systems, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in these systems may be disclosed outside Treasury as a routine use pursuant to 5 U.S.C. 552a(b)(3), as follows:

A. To the Department of Justice (including United States Attorneys' Offices) or other federal agencies conducting litigation or in proceedings before any court or adjudicative or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. Treasury or any component thereof;

2. Any employee of Treasury in his/her official capacity;

3. Any employee of Treasury in his/her individual capacity where the Department of Justice or Treasury has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office in response to an inquiry made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or General Services

Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. Treasury suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with Treasury's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, fiscal agents, financial agents, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for Treasury, when necessary to accomplish an agency function related to the system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to Treasury officers and employees.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person authorizing the disclosure.

H. To federal agencies, councils, and offices, such as the Office of Personnel Management, the Merit Systems Protection Board, the Office of Management and Budget, the Federal Labor Relations Authority, the Government Accountability Office, the Financial Stability Oversight Council, and the Equal Employment Opportunity Commission in the fulfillment of these agencies' official duties.

I. To the news media and the public, with the approval of the Senior Agency Official for Privacy, or her designee, in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of Treasury or is necessary to demonstrate the accountability of Treasury's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

K. To international, federal, state, local, tribal, or private entities for the purpose of the regular exchange of business contact information in order to facilitate collaboration for official business.

## Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

## Storage:

Records in these systems are on paper and/or in digital or other electronic form. Digital and other electronic images are stored on a storage area network in a secured environment. Records, whether paper or electronic, may be stored in Departmental Offices or with one or more contracted service providers.

## Retrievability:

Electronic information may be retrieved, sorted, and/or searched by email address, name of the individual, or other data fields previously identified in this notice.

## Safeguards:

Information in these systems is safeguarded in accordance with applicable laws, rules, and policies, including Treasury Directive 85-01, Department of the Treasury Information Technology (IT) Security Program. Further, security protocols for these systems of records will meet multiple National Institute of Standards and Technology security standards from authentication to certification and authorization. Records in these systems of records will be maintained in a secure, password protected electronic system that will use security hardware and software to include multiple firewalls, active intruder detection, and role-based access controls. Additional safeguards will vary by component and program. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a "need to know," using locks, and password protection identification features. Treasury file areas are locked after normal duty hours and the facilities are protected by security personnel who monitor access to and egress from Treasury facilities.

## Retention and disposal:

Records are securely retained and disposed in accordance with Records Control Schedule N1-056-03-010, Item 1b2. Files will be retained for ten years. For records that become relevant to litigation, the files related to that litigation will be retained for the longer of ten years or three years after final court adjudication.

## System manager(s) and address:

Deputy Assistant Secretary, Office of Tax Policy, 1500 Pennsylvania Avenue NW, Washington, DC 20220.

## Notification procedure:

Individuals seeking notification of and access to any record contained in these systems of records, or seeking to contest its content, may submit a request in writing, in accordance with Treasury's Privacy Act regulations (located at 31 CFR 1.26), to the Freedom of Information Act (FOIA) and Transparency Liaison, whose contact information can be found at *http://www.treasury.gov/FOIA/Pages/index.aspx* under "FOIA Requester Service Centers and FOIA Liaison." If an individual believes more than one bureau maintains Privacy Act records concerning him or her, the individual may submit the request to the Office of Privacy, Transparency, and Records, FOIA and Transparency, Department of the Treasury, 1500 Pennsylvania Ave. NW, Washington, DC 20220.

No specific form is required, but a request must be written and:

- Be signed and either notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization
- State that the request is made pursuant to the FOIA and/or Privacy Act disclosure regulations;
- Include information that will enable the processing office to determine the fee category of the user;

- Be addressed to the bureau that maintains the record (in order for a request to be properly received by the Department, the request must be received in the appropriate bureau's disclosure office);

- Reasonably describe the records;

- Give the address where the determination letter is to be sent;

- State whether or not the requester wishes to inspect the records or have a copy made without first inspecting them; and

- Include a firm agreement from the requester to pay fees for search, duplication, or review, as appropriate. In the absence of a firm agreement to pay, the requester may submit a request for a waiver or reduction of fees, along with justification of how such a waiver request meets the criteria for a waiver or reduction of fees found in the FOIA statute at 5 U.S.C. 552(a)(4)(A)(iii).

You may also submit your request online at *https://rdgw.treasury.gov/foia/pages/gofoia.aspx* and call 1-202-622-0930 with questions.

## Record access procedures:

See "Notification procedure" above.

## Contesting record procedures:

See "Notification procedure" above.

## Record source categories:

Information contained in these systems is obtained from affected individuals and organizations.

## Exemptions claimed for these systems:

None.

**TREASURY/DO .060**

**System name:**

Correspondence Files and Records on Dissatisfaction--Treasury/DO.

**System location:**

Office of Human Capital Strategic Management, Suite 1200, 1750 Pennsylvania Avenue, NW, Department of the Treasury, Washington, DC 20220.

**Categories of individuals covered by the system:**

Former and current Department employees who have submitted complaints to the Office of Human Resources Strategy and Solutions (HRSS) or whose correspondence concerning a matter of dissatisfaction has been referred to HRSS.

**Categories of records in the system:**

Correspondence dealing with former and current employee complaints.

**Authority for maintenance of the system:**

5 U.S.C. 301.

**Purpose(s):**

To maintain a record of correspondence related to inquiries filed with the Departmental Office of Human Resources Strategy and Solutions.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose pertinent information to appropriate federal, state, and local, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a violation or potential civil or criminal law or regulation;

(2) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(3) Provide information to unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114;

(4) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation, and

(5) To appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by bureau and employee name.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

Records are maintained and disposed of in accordance with Department of the Treasury Directive 25-02, "Records Disposition Management Program," and the General Records Schedule.

**System manager(s) and address:**

Director, Office of Human Capital Strategic Management, Suite 1200, 1750 Pennsylvania Avenue, NW, Department of the Treasury, Washington, DC 20220.

**Notification procedure:**

Persons inquiring as to the existence of a record on themselves may contact: Director, Human Capital Strategic Management, Suite 1200, 1750 Pennsylvania Avenue, NW, Department of the Treasury, Washington, DC 20220. The inquiry must include the individual's name and employing bureau.

**Record access procedures:**

Persons seeking access to records concerning themselves may contact: Office of Human Resources Strategy and Solutions, Suite 1200, 1750 Pennsylvania Avenue, NW, Department of the Treasury, Washington, DC 20220. The inquiry must include the individual's name and employing bureau.

**Contesting record procedures:**

Individuals wishing to request amendment to their records to correct factual error should contact the Director, Office of Human Resources Strategy and Solutions at the address shown in Access, above. They must furnish the following information: (a) name; (b) employing bureau; (c) the information being contested; (d) the reason why they believe information is untimely, inaccurate, incomplete, irrelevant, or unnecessary.

**Record source categories:**

Current and former employees, and/or representatives, employees' relatives, general public, Congressmen, the White House, management officials.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .120**

**System name:**

Records Related to Office of Foreign Assets Control Economic Sanctions.

**System location:**

Office of Foreign Assets Control (OFAC), Treasury Annex, 1500 Pennsylvania Ave., NW, Washington, DC 20220 or other U.S. Government facilities.

**Categories of individuals covered by the system:**

A system of records within Treasury's Departmental Offices exists to manage records related to the implementation, enforcement, and administration of U.S. economic sanctions. This includes records and information relating to individuals who:

(1) Are or have been subject to investigation to determine whether they meet the criteria for designation or blocking and/or are determined to be designated or blocked individuals or otherwise subject to sanctions under the sanctions programs administered by OFAC, or with respect to whom information has been obtained by OFAC in connection with such an investigation;

(2) Engaged in or are suspected of having engaged in transactions and activities prohibited by Treasury Department regulations found at 31 CFR part 1, subpart B, chapter V, relevant statutes, and related Executive orders or proclamations, or with respect to whom information has been obtained by OFAC in connection with an investigation of such transactions and activities;

(3) Are applicants for permissive and authorizing licenses or already hold valid licenses under Treasury Department regulations, relevant statutes, and related Executive orders or proclamations;

(4) Hold blocked assets. Although most persons (individuals and entities) reporting the holding of blocked assets or persons holding blocked assets are not individuals, such reports and

censuses conducted by OFAC identify a small number of U.S. individuals as holders of assets subject to U.S. jurisdiction which are blocked under the various sets of Treasury Department regulations involved, relevant statutes, and related Executive orders or proclamations; or

(5) Submitted claims received, reviewed, and/or processed by OFAC for payment determination pursuant to Section 2002 of the Victims of Trafficking and Violence Protection Act of 2000 (Pub. L. 106–386, Section 2002).

**Categories of records in the system:**

Records related to the implementation, enforcement, and administration of U.S. sanctions programs, including records related to:

(1) Investigations to determine whether an individual meets the criteria for designation or blocking and/or is determined to be a designated or blocked individual or otherwise affected by one or more sanctions programs administered by OFAC. In the course of an investigation, personally identifiable information is collected. Once an individual is designated, OFAC provides personally identifiable information to the public so that it can recognize listed individuals and prevent them from accessing the U.S. financial system. The release of personally identifiable information pertaining to the designee is also important in helping to protect other individuals from being improperly identified as the sanctioned target. The personally identifiable information collected by OFAC may include, but is not limited to, names and aliases, dates of birth, citizenship information, addresses, identification numbers associated with government-issued documents, such as driver's license and passport numbers, and for U.S. individuals, Social Security numbers;

(2) Suspected or actual violations of regulations, relevant statutes, and related Executive orders or proclamations administered by OFAC;

(3) Applications for OFAC licenses—with attendant supporting documentary material and copies of licenses issued—related to engaging in activities with designated entities and individuals or other activities that otherwise would be prohibited by relevant statutes, regulations, and Executive orders or proclamations administered by OFAC, including reports by individuals and entities currently holding Treasury licenses concerning transactions which the license holder has conducted pursuant to the licenses;

(4) Reports and censuses of assets blocked or held by U.S. individuals and entities which have been blocked at any time since 1940 pursuant to Treasury Department regulations found at 31 CFR part 1, subpart B, chapter V, relevant statutes, and related Executive orders or proclamations; or

(5) Submitted claims received, reviewed, and/or processed by OFAC for payment determinations pursuant to Section 2002 of the Victims of Trafficking and Violence Protection Act of 2000 (Pub. L. 106–386).

**Authority for maintenance of the system:**

3 U.S.C. 301; 50 U.S.C. App. 1–44; 21 U.S.C. 1901–1908; 8 U.S.C. 1182; 18 U.S.C. 2339B; 22 U.S.C. 287c; 31 U.S.C. 321(b); 50 U.S.C. 1601–1651; 50 U.S.C. 1701–1706; Pub. L. 110–286, 122 Stat. 2632; 22 U.S.C. 2370(a); Pub. L. 108–19, 117 Stat. 631; Pub. L. 106–386 § 2002; Pub. L. 108–175, 117 Stat. 2482; Pub. L. 109–344, 120 Stat. 1869; 31 CFR Chapter V.

**Purpose(s):**

This system of records exists within Treasury's Departmental Offices to manage records related to the implementation, enforcement, and administration of U.S. economic sanctions by OFAC. Included in this system of records are records:

(1) Relating to investigations into whether individuals and entities meet the criteria for economic sanctions under U.S. sanctions programs administered by OFAC. This portion of the system of records may be used during enforcement, designation, blocking, and other investigations, when applicable. These records are also used to produce the publicly issued List of Specially Designated Nationals and Blocked Persons (SDN List). The SDN List is used to publish information that will assist the public in identifying individuals and entities whose property and interests in property are blocked or otherwise affected by one or more sanctions programs administered by OFAC, as well as information identifying certain property of individuals and entities that are subject to OFAC economic sanctions programs, such as vessels.
(2) Relating to investigations of individuals and entities suspected of violating statutes, regulations, or Executive orders administered by OFAC. Possible violations may relate to financial, commercial, or other transactions with persons on whom sanctions have been imposed, including but not limited to foreign governments, blocked persons (entities and individuals), and specially designated nationals (entities and individuals). OFAC conducts civil investigations of possible violations. When it determines that a violation has occurred, OFAC issues a civil penalty or takes other administrative action, when appropriate. Criminal investigations of possible violations are conducted by relevant U.S. law enforcement agencies. OFAC refers criminal matters to those agencies and otherwise exchanges information with them to support the investigation and prosecution of possible violations. Records of enforcement investigations and resulting administrative actions are also used to generate statistical information. (3) Containing requests from U.S. and foreign individuals or entities for licenses to engage in commercial or humanitarian transactions, to unblock property and bank accounts, or to engage in other activities otherwise prohibited under economic sanctions administered by OFAC. This also includes

information collected in the course of determining whether to issue a license and ensuring its proper use, as well as reports by individuals and entities currently holding Treasury licenses concerning transactions which the license holder conducted pursuant to the licenses. This portion of the system of records may be used during enforcement investigations, to ascertain whether there is compliance with the conditions of ongoing OFAC licenses, and to generate information used in reports on the number and types of licenses granted or denied under particular sanctions programs.

(4) Used to identify and administer assets of blocked foreign governments, groups, entities, or individuals. OFAC receives reports of asset blocking actions by U.S. entities and individuals when assets are blocked under the sanctions programs OFAC administers; when censuses are taken at various times for specific sanctions programs to identify the location, type, and value of property blocked under OFAC-administered programs; and when OFAC obtains information regarding blockable assets in the course of its investigations. Most blocked asset information is obtained by requiring reports from all U.S. holders of blocked property subject to OFAC reporting requirements. The reports normally contain information such as the name of the U.S. holder, the account party, the location of the property, and a description of the type and value of the asset. In some instances, adverse claims by U.S. entities and individuals against the blocked property are also reported. This portion of the system of records may be used during enforcement, designation, blocking, and other investigations as well as to produce reports and respond to requests for information.

(5) Used to support determinations made by OFAC pursuant to Section 2002 of Pub. L. 106–386, the Victims of Trafficking and Violence Protection Act of 2000, including the facilitating of

payments provided for under the Act. OFAC has reported its determinations to other parts of Treasury to facilitate payment on claims.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose information to further the efforts of appropriate federal, state, local, or foreign agencies in investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or agreement;

(2) Disclose information to a federal, state, local, or foreign agency, maintaining civil, criminal, or other relevant enforcement information or other pertinent information, which has requested information necessary or relevant to the requesting agency's official functions;

(3) Disclose information to the Departments of State, Justice, Homeland Security, Commerce, Defense, or Energy, or other federal agencies, in connection with Treasury licensing policy or other matters of mutual interest or concern;

(4) Provide information to appropriate national security and/or foreign-policy-making officials in the Executive branch to ensure that the management of OFAC's sanctions programs is consistent with U.S. foreign policy and national security goals;

(5) Disclose information relating to blocked property to appropriate state agencies for activities or efforts connected to abandoned property;

(6) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosure to opposing counsel or witnesses in the course of civil

discovery, litigation, or settlement negotiations, or in response to a Court order, or in connection with criminal law proceedings, when such information is determined to be arguably relevant to the proceeding;

(7) Provide information to a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Disclose information to foreign governments and entities, and multilateral organizations—such as Interpol, the United Nations, and international financial institutions—consistent with law and in accordance with formal or informal international agreements, or for an enforcement, licensing, investigatory, or national security purpose;

(9) Provide information to third parties during the course of an investigation or an enforcement action to the extent necessary to obtain information pertinent to the investigation or to carry out an enforcement action;

(10) Provide access to information to any agency, entity, or individual for purposes of performing authorized security, audit, or oversight operations or meeting related reporting requirements;

(11) Disclose information to appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is

reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm; or

(12) Disclose information to the general public, in furtherance of OFAC's mission, regarding individuals and entities whose property and interests in property are blocked or otherwise affected by one or more OFAC economic sanctions programs, as well as information identifying certain property of individuals and entities subject to OFAC economic sanctions programs. This routine use includes disclosure of information to the general public in furtherance of OFAC's mission regarding individuals and entities that have been designated by OFAC. This routine use encompasses publishing this information in the Federal Register, in the Code of Federal Regulations, on OFAC's Web site, and by other means.

The information associated with individuals as published on OFAC's List of Specially Designated Nationals and Blocked Persons (the SDN List) generally relates to non-U.S. entities and individuals, and, therefore, the Privacy Act does not apply to most of the individuals included on the SDN List. However, a very small subset of the individuals on the SDN List consists of U.S. individuals. Individuals and entities on the SDN List are generally designated based on Executive orders and other authorities imposing sanctions with respect to terrorists, proliferators of weapons of mass destruction, sanctioned nations or regimes, narcotics traffickers, or other identified threats to the national security, foreign policy, and/or economy of the United States. Generally, the personal identifier information provided on the SDN List may include, but is not limited to, names and aliases, addresses, dates of birth, citizenship information, and, at times, identification numbers associated with government-issued documents. It is necessary to provide this identifier information in a publicly available format so that listed individuals and entities can be identified and prevented from accessing the U.S. financial system. At the same

time, the release of detailed identifier information of individuals whose property is blocked or who are otherwise affected by one or more OFAC economic sanctions programs is important in helping to protect other individuals from being improperly identified as the sanctioned target. Because the SDN List is posted on OFAC's public web site and published in the Federal Register and in 31 CFR Appendix A, a designated individual's identifier information can be accessed by any individual or entity with access to the internet, the Federal Register, or 31 CFR Appendix A. Thus, the impact on the individual's privacy will be substantial, but this is necessary in order to make targeted economic sanctions effective. Designated individuals can file a "de-listing petition" to request their removal from the SDN List. See 31 CFR 501.807. If such a petition is granted, the individual's name and all related identifier information are removed from the active SDN List.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records related to:

(1) Enforcement, designation, blocking, and other investigations are retrieved by the name of the individual or other relevant search term.

**(**2) Licensing applications are retrieved by license or letter number or by the name of the applicant.

(3) Blocked property records are retrieved by the name of the holder, custodian, or owner of blocked property.

(4) Claims received, reviewed, and processed by OFAC for payment determinations pursuant to Section 2002 of the Victims of Trafficking and Violence Protection Act of 2000, Public Law Number 106–386, are retrieved by the name of the applicant.

**Safeguards:**

Folders maintained in authorized filing equipment are located in areas of limited and controlled access and are limited to authorized Treasury employees. Computerized records are on a password-protected network. Access controls for all internal, electronic information are not less than required by the Treasury Security Manual (TDP-71-10). The published List of Specially Designated Nationals and Blocked Persons is considered public domain.

**Retention and Disposal:**

Records are managed according to applicable Federal Records Management laws and regulations (see also 5 U.S.C. Part I, Chapter 5, Subchapter II, Section 552a—Records Maintained on Individuals). Record retention and disposition rules are approved by the Archivist of the United States and applied appropriately.

**System Manager and Address:**

Director, Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Notification Procedure:**

For records in this system that are unrelated to enforcement, designation, blocking, and other investigations, individuals wishing to be notified if they are named in this system of records must submit a written request containing the following elements: (1) identify the record

system; (2) identify the category and type of record sought; and (3) provide at least two items of secondary identification (date of birth, employee identification number, dates of employment, or similar information). Address inquiries to Assistant Director, Disclosure Services, Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

For records in this system that are unrelated to enforcement, designation, blocking, and other investigations, individuals wishing to gain access to records maintained in the system under their name or personal identifier must submit a written request containing the following elements: (1) identify the record system; (2) identify the category and type of record sought; and (3) provide at least two items of secondary identification (date of birth, employee identification number, dates of employment, or similar information). Address inquiries to Assistant Director, Disclosure Services, Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220. The request must be made in accordance with 5 U.S.C. 552a and 31 CFR 1.2. See also 31 CFR part 1, subpart C, appendix A, Paragraph 8.

Records in this system that are related to enforcement, designation, blocking, and other investigations are exempt from the provisions of the Privacy Act as permitted by 5 U.S.C. 552a(k)(2). Exempt records may not be disclosed for purposes of determining if the system contains a record pertaining to a particular individual, inspecting records, or contesting the content of records. Although the investigative records that underlie the SDN List may not be accessed for purposes of inspection or for contest of content of records, the SDN List, which is produced from some of the investigative records in the system, is made public. Persons (entities

and individuals) on this public list who wish to request the removal of their name from this list may submit a de-listing petition according to the provisions of 31 CFR 501.807.

**Record access procedures:**

Address inquiries to: Assistant Director, Disclosure Services, Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Contesting record procedures:**

See "Record access procedures" above.

**Record source categories:**

(1) From the individual, from OFAC investigations, and from other federal, state, local, or foreign agencies;

(2) Applicants for Treasury Department licenses under laws or regulations administered by OFAC;

(3) From individuals and entities that are designated or otherwise subject to sanctions and the representatives of such individuals and entities; or

(4) Custodians or other holders of blocked assets.

**Exemptions claimed for the system:**

Records in this system related to enforcement, designation, blocking, and other investigations are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). See 31 CFR 1.36.

**TREASURY/DO .144**

**System name:**

General Counsel Litigation Referral and Reporting System--Treasury/DO.

**System location:**

U.S. Department of the Treasury, Office of the General Counsel, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Persons who are parties, plaintiff or defendant, in civil litigation or administrative proceedings involving or concerning the Department of the Treasury or its officers or employees. The system does not include information on every civil litigation or administrative proceeding involving the Department of the Treasury or its officers and employees.

**Categories of records in the system:**

This system of records consists of a computer data base containing information related to litigation or administrative proceedings involving or concerning the Department of the Treasury or its officers or employees.

**Authority for maintenance of the system:**

5 U.S.C. 301; 31 U.S.C. 301.

**Purpose(s):**

The purposes of this system are: (1) to record service of process and the receipt of other documents relating to litigation or administrative proceedings involving or concerning the Department of the Treasury or its officers or employees; (2) to respond to inquiries from Treasury personnel, personnel from the Justice Department and other agencies, and other persons concerning whether service of process or other documents have been received by the Department

in a particular litigation or proceeding; and (3) to keep track of the specific Treasury component assigned to handle a particular litigation or administrative matter.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose information to the Department of Justice (including United States Attorneys' Offices) or other federal agencies conducting litigation or in proceedings before any court or adjudicative or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

a. Treasury or any component thereof;

b. Any employee of Treasury in his/her official capacity;

c. Any employee of Treasury in his/her individual capacity where the Department of Justice or Treasury has agreed to represent the employee; or

d. The United States or any agency thereof.

(2) Disclose pertinent information to appropriate federal, state, or foreign agencies responsible for investigating or prosecuting the violations of, or for implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(3) Disclose information to a federal, state, or local agency, maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations in response to a court order or in connection with criminal law proceedings;

(5) Disclose information to foreign governments in accordance with formal or informal international agreements;

(6) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(7) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation, and

(8) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by the name of the non-government party involved in the case, and case number and docket number (when available).

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. Also, Background checks are made on employees.

**Retention and disposal:**

The computer information is maintained for up to ten years or more after a record is created.

**System manager(s) and address:**

Office of General Law, Ethics & Regulation, Office of the General Counsel, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, or gain access to records maintained in this system must submit a written request containing the following elements: (1) an identification of the record system; and (2) an identification of the

category and type of records sought. This system contains records that are exempt under 31 CFR 1.36; 5 U.S.C. 552a(j)(2); and (k)(2). Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Record access procedures:**

Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedures:**

See "Record access procedures" above.

**Record source categories:**

Treasury Department Legal Division, Department of Justice Legal Division.

**Exemptions claimed for the system:**

This system is exempt from 5 U.S.C. 552a(d), (e)(1), (e)(3), (e)(4)(G), (H), (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). (See 31 CFR 1.36)

**TREASURY/DO .149**

**System name:**

Foreign Assets Control Legal Files--Treasury/DO.

**System location:**

U.S. Department of the Treasury, Office of the Chief Counsel (Foreign Assets Control), 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Persons who are or who have been parties in litigation or other matters involving the Office of Foreign Assets Control (OFAC) or involving statutes and regulations administered by the OFAC found at 31 CFR subtitle B, chapter V.

**Categories of records in the system:**

Information and documents relating to litigation and other matters involving the OFAC or statutes and regulations administered by the OFAC.

**Authority for maintenance of the system:**

31 U.S.C. 301; 50 U.S.C. App. 5(b); 50 U.S.C. 1701 et seq.; 22 U.S.C. 287(c); and other statutes relied upon by the President to impose economic sanctions.

**Purpose(s):**

These records are maintained to assist in providing legal advice to the OFAC and the Department of the Treasury regarding issues of compliance, enforcement, investigation, and implementation of matters related to OFAC and the statutes and regulations administered by the agency. These records are also maintained to assist in litigation related to OFAC and the statutes and regulations administered by the OFAC.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Prosecute, defend, or intervene in litigation related to the OFAC and statutes and regulations administered by OFAC,

(2) Disclose pertinent information to appropriate federal, state, local, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license;

(3) Disclose information to a federal, state, or local agency, maintaining civil, criminal, or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's official functions;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings;
(5) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains, and
(6) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name of the non-government party involved in the matter.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

Records are periodically updated and maintained as long as needed.

**System manager(s) and address:**

Office of Chief Counsel, Foreign Assets Control, U.S. Treasury Department, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, or gain access to records maintained in this system must submit a written request containing the following elements: (1) Identify the record system; (2) identify the category and type of records sought; and (3) provide identification as set forth in 31 CFR Subpart C, Part 1, Appendix A, Section 8.

**Record access procedures:**

Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedures:**

See “Record access procedures” above.

**Record source categories:**

Pleadings and other materials filed during course of a legal proceeding, discovery obtained pursuant to applicable court rules; materials obtained by Office of Foreign Assets Control action; material obtained pursuant to requests made to other Federal agencies; orders, opinions, and decisions of courts.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .190**

**System name:**

Office of Inspector General Investigations Management Information System--Treasury/DO.

**System location:**

Office of Inspector General (OIG), Assistant Inspector General for Investigations and Counsel to the Inspector General, 740 15th St., NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

(A) Current and former employees of the Department of the Treasury and persons whose association with current and former employees relate to the alleged violations of the rules of ethical conduct for employees of the Executive Branch, the Department’s supplemental standards of ethical conduct, the Department’s rules of conduct, merit system principles, or any other

criminal or civil misconduct, which affects the integrity or facilities of the Department of the Treasury. The names of individuals and the files in their names may be: (1) received by referral; or (2) initiated at the discretion of the Office of Inspector General in the conduct of assigned duties. Investigations of allegations against OIG employees are managed by the Deputy Inspector General and the Counsel to the Inspector General; records are maintained in the Office of General Counsel.

(B) Individuals who are: witnesses; complainants; confidential or non-confidential informants; suspects; defendants; parties who have been identified by the Office of Inspector General, constituent units of the Department of the Treasury, other agencies, or members of the general public in connection with the authorized functions of the Inspector General.

(C) Current and former senior Treasury and bureau officials who are the subject of investigations initiated and conducted by the Office of the Inspector General.

**Categories of records in the system:**

(A) Letters, memoranda, and other documents citing complaints of alleged criminal or administrative misconduct. (B) Investigative files which include: (1) reports of investigations to resolve allegations of misconduct or violations of law with related exhibits, statements, affidavits, records or other pertinent documents obtained during investigations; (2) transcripts and documentation concerning requests and approval for consensual telephone and consensual non-telephone monitoring; (3) reports from or to other law enforcement bodies; (4) prior criminal or noncriminal records of individuals as they relate to the investigations; and (5) reports of actions taken by management personnel regarding misconduct and reports of legal actions resulting from violations of statutes referred to the Department of Justice for prosecution.

**Authority for maintenance of the system:**

The Inspector General Act of 1978, as amended, 5 U.S.C.A. App.3; 5 U.S.C. 301; 31 U.S.C. 321.

**Purpose(s):**

The records and information collected and maintained in this system are used (a) to receive allegations of violations of the standards of ethical conduct for employees of the Executive Branch (5 CFR part 2635), the Treasury Department's supplemental standards of ethical conduct (5 CFR part 3101), the Treasury Department's rules of conduct (31 CFR part 0), the Office of Personnel Management merit system principles, or any other criminal or civil law; and (b) to prove or disprove allegations which the OIG receives that are made against Department of the Treasury employees, contractors and other individuals associated with the Department of the Treasury.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose information to the Department of Justice in connection with actual or potential criminal prosecution or civil litigation;

(2) Disclose pertinent information to appropriate federal, state, local, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, or where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(3) Disclose information to a federal, state, or local agency, maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's hiring or retention of an employee, or the issuance of a security clearance, license, contract, grant, or other benefit;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation or settlement negotiations in response to a court order or in connection with criminal law proceedings;

(5) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(6) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2 which relate to an agency's functions relating to civil and criminal proceedings;

(7) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(8) Provide information to the Office of Inspector General of the Department of Justice with respect to investigations involving the former Bureau of Alcohol, Tobacco, and Firearms; and to the Office of Inspector General of the Department of Homeland Security with respect to investigations involving the Secret Service, the former Customs Service, and Federal Law Enforcement Training Center, for such OIG's use in carrying out their obligations under the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3 and other applicable laws;

(9) Provide information to other OIGs, the Council of Inspectors General on Integrity and Efficiency, and the Department of Justice, in connection with their review of Treasury OIG's

exercise of statutory law enforcement authority, pursuant to section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3; and

(10) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved alphabetically by name of subject or complainant, by case number, by special agent name, by employee identifying number, by victim, and by witness case number.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The records are available to Office of Inspector General personnel who have an appropriate security clearance on a need-to-know basis.

**Retention and disposal:**

Investigative records are stored on-site for 3 years at which time they are retired to the Federal Records Center, Suitland, Maryland, for temporary storage. In most instances, the files are destroyed when 10 years old. However, if the records have significant or historical value, they are retained on-site for 3 years, then retired to the Federal Records Center for 22 years, at which time they are transferred to the National Archives and Records Administration for permanent retention. In addition, an automated investigative case tracking system is maintained on-site; the case information deleted 15 years after the case is closed, or when no longer needed, whichever is later.

**System manager(s) and address:**

Assistant Inspector General for Investigations, 740 15th St., NW, Suite 500, Washington, DC 20220. For internal investigations: Counsel to the Inspector General, 740 15th St., NW, Suite 510, Washington, DC 20220.

**Notification procedure:**

Pursuant to 5 U.S. C. 552a(j)(2) and (k)(2), this system of records may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual, or for contesting the contents of a record.

**Record Access procedures:**

See "Notification procedure" above.

**Contesting Record procedures:**

See "Notification procedure" above.

**Record source categories:**

See "Categories of individuals" above. This system contains investigatory material for which sources need not be reported.

**Exemptions claimed for the system:**

This system is exempt from 5 U.S.C. 552a(c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). See 31 CFR 1.36.

**TREASURY/DO .191**

**System name:**

Human Resources and Administrative Records System.

**System location:**

Office of Inspector General (OIG), headquarters and Boston field office.

(See appendix A)

**Categories of individuals covered by the system:**

(A) Current and former employees of the Office of Inspector General.

(B) Individuals who are: witnesses; complainants; confidential or non-confidential informants; suspects; defendants; parties who have been identified by the Office of Inspector General, constituent units of the Department of the Treasury, other agencies, or members of the general public, in connection with the authorized functions of the Inspector General.

**Categories of records in the system:**

(1) Personnel system records contain OIG employee name, positions, grade and series, salaries, and related information pertaining to OIG employment; (2) Tracking records contain status information on audits, investigations and other projects; (3) Timekeeping records contain hours worked and leave taken; (4) Equipment inventory records contain information about government property assigned to employees.

**Authority for maintenance of the system:**

Inspector General Act of 1978, as amended; (5 U.S.C. Appendix 3) 5U.S.C. 301; and 31 U.S.C. 321.

**Purpose(s):**

The purpose of the system is to: (1) effectively manage OIG resources and projects; (2) capture accurate statistical data for mandated reports to the Secretary of the Treasury, the Congress, the Office of Management and Budget, the Government Accountability Office, the Council of the Inspectors General on Integrity and Efficiency and other Federal agencies; and (3) provide accurate information critical to the OIG's daily operation, including employee performance and conduct; and (4) collect and maintain information provided to the OIG concerning violation of any criminal or civil law made against or regarding individuals associated or claiming association with the Department of the Treasury.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

(1) A record from the system of records, which indicates, either by itself or in combination with other information, a violation or potential violation of law, whether civil or criminal, and whether arising by statute, regulation, rule or order issued pursuant thereto, may be disclosed to a federal, state, local, or foreign agency or other public authority that investigates or prosecutes or assists in investigation or prosecution of such violation, or enforces or implements or assists in enforcement or implementation of the statute, rule, regulation or order; or to any private entity in order to prevent loss or damage to any party by reason of false or fictitious financial instruments or documents.

(2) A record from the system of records may be disclosed to a federal, state, local, or foreign agency or other public authority, or to private sector (i.e., non-federal, State, or local government) agencies, organizations, boards, bureaus, or commissions, which maintain civil, criminal, or other relevant enforcement records or other pertinent records, such as current licenses in order to obtain information relevant to an agency investigation, audit, or other inquiry, or relevant to a decision concerning the hiring or retention of an employee or other personnel action, the issuance of a security clearance, the letting of a contract, the issuance of a license, grant or other benefit, the establishment of a claim, or the initiation of administrative, civil, or criminal action. Disclosure to the private sector may be made only when the records are properly constituted in accordance with agency requirements; are accurate, relevant, timely and complete; and the disclosure is in the best interest of the Government.

(3) A record from the system of records may be disclosed to a federal, state, local, or foreign agency or other public authority, or private sector (i.e., non-federal, state, or local government)

agencies, organizations, boards, bureaus, or commissions, if relevant to the recipient's hiring or retention of an employee or other personnel action, the issuance of a security clearance, the letting of a contract, the issuance of a license, grant or other benefit, the establishment of a claim, or the initiation of administrative, civil, or criminal action. Disclosure to the private sector may be made only when the records are properly constituted in accordance with agency requirements; are accurate, relevant, timely and complete; and the disclosure is in the best interest of the Government.

(4) A record from the system of records may be disclosed to any source, private or public, to the extent necessary to secure from such source information relevant to a legitimate agency investigation, audit, or other inquiry.

(5) A record from the system of records may be disclosed to the Department of Justice when the agency or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

(6) A record from the system of records may be disclosed in a proceeding before a court or adjudicative body, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency

determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

(7) A record from the system of records may be disclosed to a Member of Congress from the record of an individual in response to an inquiry from the Member of Congress made at the request of that individual.

(8) A record from the system of records may be disclosed to the Department of Justice and the Office of Government Ethics for the purpose of obtaining advice regarding a violation or possible violation of statute, regulation, rule or order or professional ethical standards.

(9) A record from the system of records may be disclosed to the Office of Management and Budget for the purpose of obtaining its advice regarding agency obligations under the Privacy Act, or in connection with the review of private relief legislation.

(10) A record from the system of records may be disclosed in response to a court order issued by a federal agency having the power to subpoena records of other Federal agencies if, after careful review, the OIG determines that the records are both relevant and necessary to the requesting agency's needs and the purpose for which the records will be used is compatible with the purpose for which the records were collected.

(11) A record from the system of records may be disclosed to a private contractor for the purpose of compiling, organizing, analyzing, programming, or otherwise refining records subject to the same limitations applicable to U.S. Department of the Treasury officers and employees under the Privacy Act.

(12) A record from the system of records may be disclosed to a grand jury agent pursuant either to a federal or state grand jury subpoena, or to a prosecution request that such record be released for the purpose of its introduction to a grand jury provided that the Grand Jury channels its request through the cognizant U.S. Attorney, that the U.S. Attorney is delegated the authority to make such requests by the Attorney General, that she or he actually signs the letter specifying both the information sought and the law enforcement purposes served. In the case of a State Grand Jury subpoena, the State equivalent of the U.S. Attorney and Attorney General shall be substituted.

(13) A record from the system of records may be disclosed to a federal agency responsible for considering suspension or debarment action where such record would be relevant to such action.

(14) A record from the system of records may be disclosed to an entity or person, public or private, where disclosure of the record is needed to enable the recipient of the record to take action to recover money or property of the United States Department of the Treasury, where such recovery will accrue to the benefit of the United States, or where disclosure of the record is needed to enable the recipient of the record to take appropriate disciplinary action to maintain the integrity of the programs or operations of the Department of the Treasury.

(15) A record from the system of records may be disclosed to a federal, state, local or foreign agency, or other public authority, for use in computer matching programs to prevent and detect fraud and abuse in benefit programs administered by an agency, to support civil and criminal law enforcement activities of any agency and its components, and to collect debts and over payments owed to any agency and its components.

(16) A record from the system of records may be disclosed to a public or professional licensing organization when such record indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

(17) A record from the system of records may be disclosed to the Office of Management and Budget, the Government Accountability Office, the Council of the Inspectors General on Integrity and Efficiency and other Federal agencies for mandated reports.

(18) Disclosures are not made outside of the Department, except to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Disclosure to consumer reporting agencies:**

Debtor information may also be furnished, in accordance with 5 U.S.C. 552a(b)(12) and 31 U.S.C. 3711(e) to consumer reporting agencies to encourage repayment of an overdue debt.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locker door. Electronic records are stored in magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Most files are accessed by OIG employee name, employee identifying number, office, or cost center. Some records may be accessed by entering equipment or project information. Financial instrument fraud database information may be accessed by name and address.

**Safeguards:**

Access is limited to OIG employees who have a need for such information in the course of their work. Offices are locked. A central network server is password protected by account name and user password. Access to records on electronic media is controlled by computer passwords. Access to specific system records is further limited and controlled by computer security programs limiting access to authorized personnel.

**Retention and disposal:**

Records are periodically updated to reflect changes and are retained as long as necessary.

**System manager(s) and address:**

Assistant Inspector General for Management, 740 15th St. NW, Suite 510, Washington, DC 20220. For records provided by the general public concerning financial instrument fraud: Counsel to the Inspector General, 740 15th St., NW, Suite 510, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, or to gain access to records maintained in this system may inquire in accordance with instructions appearing in 31 CFR part 1, subpart C, appendix A. Individuals must submit a written request containing the following elements: (1) identify the record system; (2) identify the category and type of records sought; and (3) provide at least two items of secondary identification (date of birth, employee identifying number, dates of employment, or similar information). Address inquiries to Director, Disclosure Services (see "Record access procedures" below).

**Record access procedures:**

Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedure:**

See "Record access procedures" above.

**Record source categories:**

Current and former employees of the OIG; persons providing information concerning or alleged to be committing financial instrument fraud.

**Exemptions claimed for the system:**

None.

**Appendix A--Addresses of OIG Offices**

Headquarters:

Department of the Treasury, Office of Inspector General, Office of the Assistant Inspector General for Management, 740 15th Street, NW, Suite 510, Washington, DC 20220.

Field Location:

Contact System Manager for addresses.

Department of the Treasury, Office of Inspector General, Office of Audit, Boston, MA 02110-3350.

**TREASURY/DO .193**

**System name:**

Employee Locator and Automated Directory System--Treasury/DO.

**System location:**

Main Treasury Building, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Information on all employees of the Department is maintained in the system if the proper locator card is provided.

**Categories of records in the system:**

Name, office telephone number, bureau, office symbol, building, room number, home address and phone number, and person to be notified in case of emergency.

**Authority for maintenance of the system:**

5 U.S.C. 301.

**Purpose(s):**

The Employee Locator and Automated Directory System is maintained for the purpose of providing current locator and emergency information on all DO employees.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosures are not made outside of the Department, except to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls

have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearance or permissions.

**Retention and disposal:**

Records are kept as long as needed, updated periodically and destroyed by burning.

**System manager(s) and address:**

Manager, Telephone Operator Services Branch, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

See "System manager" above.

**Record Access procedures:**

See "System manager" above.

**Contesting Record procedures:**

See "System manager" above.

**Record source categories:**

Information is provided by individual employees. Necessary changes made if requested.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .194**

**System name:**

Circulation System--Treasury.

**System location:**

Department of the Treasury, Library, Room 1428-MT, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Employees who borrow library materials or receive library materials on distribution. The system also contains records concerning interlibrary loans to local libraries which are not subject to the Privacy Act.

**Categories of records in the system:**

Records of items borrowed from the Treasury Library collection and patron records are maintained on a central computer. Records are maintained by name of borrower, office locator information, and title of publication.

**Authority for maintenance of the system:**

5 U.S.C. 301.

**Purpose(s):**

Track circulation of library materials and their borrowers.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

(1) These records may be used to disclose information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains; and

(2) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been

compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by borrower name, bar code number, publication title, or its associated bar code number.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

Only current data are maintained on-line. Records for borrowers are deleted when the employee leaves Treasury.

**System manager(s) and address:**

Chief Librarian, Department of the Treasury, Room 1428-MT, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

Inquiries should be addressed to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington DC 20220.

**Record Access procedures:**

See "Notification procedure" above.

**Contesting Record procedures:**

See "Notification procedure" above.

**Record source categories:**

Patron information records are completed by borrowers and library staff.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .196**

**System name:**

Treasury Information Security Program--Treasury/DO.

**System location:**

Department of the Treasury, Office of Security Programs, Room 3180 Treasury Annex, 1500 Pennsylvania Avenue NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

(1) Each Department of the Treasury official, by name and position title, who has been delegated the authority to downgrade and declassify national security information and who is not otherwise authorized to originally classify.

(2) Each Department of the Treasury official, by name and position title, who has been delegated the authority for original classification of national security information, exclusive of officials specifically given this authority via Treasury Order 105-19.

(3) Department of the Treasury employees who have valid security violations as a result of the improper handling/processing, safeguarding or storage of classified information or collateral national security systems.

(4) Department of the Treasury employees (including detailees, interns and select contractors) who receive initial, specialized and/or annual refresher training on requirements for protecting classified information.

(5) Department of the Treasury employees and contractors issued a courier card authorizing them to physically transport classified information within and between Treasury, bureaus, and other U.S. Government agencies and departments.

(6) Departmental Offices officials and bureau heads issued Department of the Treasury credentials as evidence of their authority and empowerment to execute and fulfill the duties of their appointed office and those Departmental Offices officials authorized to conduct official investigations and/or inquiries on behalf of the U.S. Government.

**Categories of records in the system:**

(1) Report of Authorized Downgrading and Declassification Officials, (2) Report of Authorized Classifiers, (3) Record of Security Violation, (4) Security Orientation Acknowledgment, (5) Request and Receipt for Courier Card, and (6) Request and Receipt for Official Credential.

**Authority for maintenance of the system:**

Executive Order 13526, dated December 29, 2009 and the Treasury Security Manual, TD P 15-71, last updated October 28, 2011.

**Purpose(s):**

The system is designed to (1) oversee compliance with Executive Order 13526, Information Security Oversight Office Directives, the Treasury Security Manual, and Departmental security programs, (2) ensure proper classification of national security information, (3) record details of valid security violations, (4) assist in determining the effectiveness of information security programs affecting classified and sensitive information, and (5) safeguard classified information throughout its entire life-cycle.

**Routine uses of records maintained in the system, including categories of users and the purpose of such uses:**

These records may be used to disclose pertinent information to:

(1) Appropriate Federal agencies responsible for the protection of national security information, or reporting a security violation of, or enforcing, or implementing, a statute, rule, regulation, or order, or where the Department becomes aware of an indication of a potential violation of civil or criminal law or regulation, rule or order;

(2) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(3) Another federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the Federal Government is a party to the judicial or administrative proceeding. In those cases where the Federal Government is not a party to the proceeding, records may be disclosed if a subpoena has been signed by a court of competent jurisdiction;

(4) The United States Department of Justice for the purpose of representing or providing legal advice to the Treasury Department (Department) in a proceeding before a court, adjudicative body, or other administrative body before which the Department is authorized to appear, when such proceeding involves:

(A) The Department or any component thereof;

(B) Any employee of the Department in his or her official capacity;

(C) Any employee of the Department in his or her individual capacity where the Department of Justice or the Department has agreed to represent the employee; or

(D) The United States, when the Department determines that litigation is likely to affect the Department or any of its components, and

(5) Appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been

compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise that there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Electronic media and hard copy files.

**Retrievability:**

Records may be retrieved by the name of the official or employee, contractor, detailee or intern, bureau head and/or chief deputy official and position title, where appropriate.

**Safeguards:**

Secured in security containers and/or controlled space to which access is limited to Office of Security Programs security officials with the need to know.

**Retention and disposal:**

Records are retained and disposed of in accordance with General Records Schedule 18, with the exception of the Record of Security Violation (retained for a period of two years) and the Security Orientation Acknowledgment, the Request and Receipt for Courier Card, and the Request and Receipt for Official Credential, the remaining records are destroyed and/or updated

on an annual basis. Destruction is effected by on-site shredding or other comparable means.

**System manager(s) and address:**

Assistant Director, (Information Security), Office of Security Programs, Room 3180 Treasury Annex, 1500 Pennsylvania Avenue NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, gain access to records maintained in this system, or seek to contest its content, must submit a written request containing the following elements: (1) identify the record system; (2) identify the category and type of records sought; and (3) provide at least two items of secondary identification (See 31 CFR Part 1, Appendix A). Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave. NW, Washington, DC 20220.

**Record access procedures:**

See "notification procedure" above.

**Contesting record procedures:**

See "Record access procedures" above.

**Record source categories:**

The sources of the information are employees of the Department of the Treasury. The information concerning any security violation is reported by Department of the Treasury security officials and by Department of State security officials as concerns Treasury or bureau personnel assigned to overseas U.S. diplomatic posts or missions.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .202**

**System name:**

Drug-Free Workplace Program Records--Treasury/DO.

**System location:**

Records are located within the Office of Human Capital Strategic Management, Room 5224-MT, Department of the Treasury, Departmental Offices, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Employees of Departmental Offices.

**Categories of records in the system:**

Records related to selection, notification, testing of employees, drug test results, and related documentation concerning the administration of the Drug-Free Workplace Program within Departmental Offices.

**Authority for maintenance of the system:**

Pub. L. 100-71; 5 U.S.C. 7301 and 7361; 21 U.S.C. 812; Executive Order 12564, "Drug-Free Federal Workplace".

**Purpose(s):**

The system has been established to maintain records relating to the selection, notification, and testing of Departmental Offices' employees for use of illegal drugs and drugs identified in Schedules I and II of 21 U.S.C. 812.

**Routine uses of records maintained in the system, including categories of users and the purpose of such uses:**

(1) these records may be disclosed to a court of competent jurisdiction where required by the United States Government to defend against any challenge against any adverse personnel action, and

(2) to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name of employee, position, title, social security number, I.D. number (if assigned), or any combination of these.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. Procedural and documentary requirements of Public Law 100-71 and the Department of Health and Human Services Guidelines will be followed.

**Retention and disposal:**

Records are retained for two years and then destroyed by shredding, or, in case of magnetic media, erasure. Written records and test results may be retained up to five years or longer when necessary due to challenges or appeals of adverse action by the employee.

**System manager(s) and address:**

Director, Office of Human Capital Strategic Management, Department of the Treasury, 1500 Pennsylvania Ave., NW, Room 5224-MT, Washington, DC 20220.

**Notification procedure:**

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the attention of the Director, Disclosure Services, Departmental Offices, 1500 Pennsylvania Ave., NW, Washington, DC 20220. Individuals must furnish their full name, Social Security Number, the title, series and grade of the position they occupied, the month and year of any drug test(s) taken, and verification of identity as required by 31 CFR part 1, subpart C, appendix A.

**Record Access procedures:**

Individuals seeking to determine whether this system of records contains information about them should address written inquiries to the attention of the Director, Disclosure Services, Departmental Offices, 1500 Pennsylvania Ave., NW, Washington, DC 20220. Individuals must furnish their full name, Social Security Number, the title, series and grade of the position they occupied, the month and year of any drug test(s) taken, and verification of identity as required by 31 CFR part 1, subpart C, appendix A.

**Contesting records procedures:**

The Department of the Treasury rules for accessing records, for contesting contents, and appealing initial determinations by the individual concerned are published in 31 CFR part 1, subpart A, appendix A.

**Record source categories:**

Records are obtained from the individual to whom the record pertains; Departmental Offices employees involved in the selection and notification of individuals to be tested; contractor laboratories that test urine samples for the presence of illegal drugs; Medical Review Officers; supervisors and managers and other Departmental Offices official engaged in administering the Drug-Free Workplace Program; the Employee Assistance Program, and processing adverse actions based on drug test results.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .207**

**System name:**

Waco Administrative Review Group Investigation--Treasury/DO.

**System location:**

Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

(A) Individuals who were employees or former employees of the Department of the Treasury and its bureaus and persons whose associations with current and former employees relate to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas on February 28, 1993, or any other criminal or civil misconduct, which affects the integrity or facilities of the Department of the Treasury. The names of individuals and the files in their names may be: (1) received by referral; or (2) developed in the course of the investigation.

(B) Individuals who were: witnesses; complainants; confidential or non-confidential informants; suspects; defendants who have been identified by the former Office of Enforcement, constituent units of the Department of the Treasury, other agencies, or members of the general public in connection with the authorized functions of the former Office of Enforcement.

(C) Members of the general public who provided information pertinent to the investigation.

**Categories of records in the system:**

(A) Letters, memoranda, and other documents citing complaints of alleged criminal misconduct pertinent to the events leading to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993.

(B) Investigative files that include:

(1) Reports of investigations to resolve allegations of misconduct or violations of law and to comply with the President's specific directive for a fact finding report on the events leading to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993, with related exhibits, statements, affidavits, records or other pertinent documents obtained during investigation;

(2) Transcripts and documentation concerning requests and approval for consensual telephone and consensual non-telephone monitoring;

(3) Reports from or to other law enforcement bodies;

(4) Prior criminal or noncriminal records of individuals as they relate to the investigations;

(5) Reports of actions taken by management personnel regarding misconduct and reports of legal actions resulting from violations of statutes referred to the Department of Justice for prosecution;

(6) Videotapes of events pertinent to the events leading to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993, or to the Department of Justice criminal prosecutions;

(7) Audiotapes with transcripts of events pertinent to the events leading to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993, or to the Department of Justice criminal prosecutions;

(8) Photographs and blueprints pertinent to the events leading to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993, or to the Department of Justice criminal

prosecutions; and

(9) Drawings, sketches, models portraying events pertinent to the events leading to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993, or to the Department of Justice criminal prosecutions.

**Purpose(s):**

The purpose of the system of records was to implement a database containing records of the investigation conducted by the Waco Administrative Review Group, and other relevant information with regard to the events leading to the former Bureau of Alcohol, Tobacco & Firearms execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993, and, where appropriate, to disclose information to other law enforcement agencies that have an interest in the information.

**Authority for maintenance of the system:**

5 U.S.C. 301; 31 U.S.C. 321.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose information to the Department of Justice in connection with actual or potential criminal prosecution or civil litigation;

(2) Disclose pertinent information to appropriate federal, state, local, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, or where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(3) Disclose information to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information that has requested information relevant to or necessary to the requesting agency's hiring or retention of an employee, or the issuance of a security clearance, license, contract, grant, or other benefit;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations in response to a court order, where relevant and necessary, or in connection with criminal law proceedings;

(5) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(6) Provide a report to the President and the Secretary of the Treasury detailing the investigation and findings concerning the events leading to the former Bureau of Alcohol, Tobacco & Firearms' execution of search and arrest warrants at the Branch Davidian compound, near Waco, Texas, on February 28, 1993, and

(7) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved alphabetically by name, by number, or other alpha-numeric identifiers.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

Investigative files are stored on-site for six years and indices to those files are stored on-site for ten years. The word processing disks will be retained indefinitely, and to the extent required they will be updated periodically to reflect changes and will be purged when the information is no longer required. Upon expiration of their respective retention periods, the

investigative files and their indices will be transferred to the Federal Records Center, Suitland, Maryland, for storage and in most instances destroyed by burning, maceration or pulping when 20 years old. The files are no longer active.

**System manager(s) and address:**

Department of the Treasury official prescribing policies and practices: Office of the Under Secretary for Enforcement, Room 4312-MT, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking access to any record contained in the system of records, or seeking to contest its content, may inquire in accordance with instructions appearing at 31 CFR part 1, subpart c, appendix A. Inquiries should be directed to the Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Record access procedures:**

See "Notification procedure" above.

**Contesting record procedures:**

See "Notification procedure" above.

**Record source categories:**

Individuals who were witnesses; complainants; confidential or non-confidential informants; suspects; defendants, constituents of the Department of the Treasury, other federal, state, or local agencies and members of the public.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .209**

**System name:**

Personal Services Contracts (PSCs)--Treasury/DO.

**System location:**

(1) Office of Technical Assistance, Department of the Treasury, 740 15th Street, NW, Washington, DC 20005.

(2) Procurement Services Division, Department of the Treasury, Mail stop: 1425 New York Ave., Suite 2100, 1500 Pennsylvania Ave, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Individuals who have been candidates or were awarded a personal services contract (PSC) with the Department of the Treasury.

**Categories of records in the system:**

Name, address, telephone number, demographic data, education, contracts, supervisory notes, personnel related information, financial, payroll and medical data and documents pertaining to the individual contractors.

**Authority for maintenance of the system:**

Support for Eastern European Democracy (SEED) Act of 1989 (Pub. L. 101-179), Freedom Support Act (Pub. L. 102-511), Executive Order 12703.

**Purpose(s):**

To maintain records pertaining to the awarding of personal services contracts to individuals for the provision of technical services in support of the SEED Act and the FSA, and which establish an employer/employee relationship with the individual.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to disclose:

(1) Pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority, responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(2) Information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(3) Information to a federal, state, local, or other public authority maintaining civil, criminal, or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(4) Information in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear when: (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee; or (d) the United States, when the agency determines that litigation is likely to affect the agency, is party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(5) Information to a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains; and

(6) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name of the individual contractor and contract number.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored.

Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearance or permissions.

**Retention and disposal:**

Records are periodically updated when a contract is modified. Contract records, including all biographical or other personal data, are retained for the contract period, with disposal after contract completion in accordance with the Federal Acquisition Regulation 4.805.

**System manager(s) and address:**

(1) Director, Office of Technical Assistance, Department of the Treasury, 740 15th Street, NW, Washington, DC 20005.

(2) Director, Procurement Services Division, Department of the Treasury, Mail stop: 1425 New York Ave, Suite 2100, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, or to gain access or seek to contest its contents, may inquire in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Inquiries should be addressed to the Director, Disclosure Services, Departmental Offices, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Record access procedures:**

See “Notification procedure” above.

**Contesting record procedures:**

See “Notification procedures” above.

**Record source categories:**

Information is provided by the candidate, individual Personal tractor, and Treasury employees.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .214**

**System name:**

DC Pensions Retirement Records.

**System Location:**

Office of DC Pensions, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220. Electronic and paper records are also located at the offices of the District of Columbia government and bureaus of the Department, including the Bureau of the Fiscal Service in Parkersburg, WV, and in Kansas City, MO. In addition, certain records are located with contractors engaged by the Department.

**Categories of individuals covered by the system:**

(A) Current and former District of Columbia police officers, firefighters, teachers, and judges.

(B) Surviving spouses, domestic partners, children, and/or dependent parents of current and former District of Columbia police officers, firefighters, teachers, or judges, as applicable.

(C) Former spouses and domestic partners of current and former District of Columbia police officers, firefighters, teachers, or judges, as applicable.

(D) Designated beneficiaries of items a, b, and c.

**Categories of records in the system:**

The categories of records include, but are not limited to, identifying information such as: name(s); contact information; Social Security number; employee identification number; service beginning and end dates; annuity beginning and end dates; date of birth; sex; retirement plan; base pay; average base pay; final salary; type(s) of service and dates used to compute length of service; military base pay amount; purchase of service calculation and amount; and/or benefit payment amount(s). The types of records in the system may be:

(a) Documentation comprised of service history/credit, personnel data, retirement contributions, and/or a refund claim upon which a benefit payment(s) may be based.

(b) Medical records and supporting evidence for disability retirement applications and continued eligibility, and documentation regarding the acceptance or rejection of such applications.

(c) Records submitted by a surviving spouse, a child(ren), and/or a dependent parent(s) in support of claims to a benefit payment(s).

(d) Consent forms and other records related to the withholding of income tax from a benefit payment(s).

(e) Retirement applications, including supporting documentation, and acceptance or denial of such applications.

(f) Death claim, including supporting documentation, submitted by a surviving spouse, child(ren), former spouse, and/or beneficiary, that is required to determine eligibility for and receipt of a benefit payment(s), or denial of such claims.

(g) Documentation of enrollment and/or change in enrollment for health and life insurance benefits/eligibility.

(h) Designation(s) of a beneficiary(ies) for a life insurance benefit and/or an unpaid benefit payment.

(i) Court orders submitted by former spouses or domestic partners in support of claims to a benefit payment(s).

(j) Records relating to under- and/or over-payments of benefit payments and other debts arising from the responsibility to administer the retirement plans for District police officers, firefighters, teachers, and judges; and, records relating to other federal debts owed by recipients of federal benefit payments. Records relating to the refunds of employee contributions.

(k) Records relating to child support orders, bankruptcies, tax levies, and garnishments.

(l) Records used to determine a total benefit payment and/or if the benefit payment is a District or federal liability.

(m) Correspondence received from current and former police officers, firefighters, teachers, and judges; including their surviving spouses, domestic partners, children, former spouses, dependent parents, and/or beneficiaries as applicable.

(n) Records relating to time served on behalf of a recognized labor organization.

(o) Records relating to benefit payment enrollment and/or change to enrollment for direct deposit to an individual's financial institution.

(p) Records submitted by a beneficiary in support of claims to a benefit payment.

(q) Records relating to educational program enrollments of age 18 and older children of former police officers, firefighters, teachers, and judges.

(r) Records related to the mental or physical handicap condition of age 18 and older children of former police officers, firefighters, teachers, and judges.

**Authority for maintenance of the system:**

Title XI, subtitle A, chapters 1 through 9, and subtitle C, chapter 4, subchapter B of the Balanced Budget Act of 1997 (as amended), Pub L. No. 105-33.

**Purpose(s):**

These records may provide information on which to base determinations of (1) eligibility for, and computation of, benefit payments and refund of contribution payments; (2) direct deposit elections into a financial institution; (3) eligibility and premiums for health insurance and group life insurance; (4) withholding of income taxes; (5) under- or over-payments to recipients of a benefit payment, and for overpayments, the recipient's ability to repay the overpayment; (6) federal payment made from the General Fund to the District of Columbia Pension Fund and the District of Columbia Judicial Retirement and Survivors Annuity Fund (Funds); (7) impact to the Funds due to proposed federal and/or District legislative changes; and (8) District or federal liability for benefit payments to former District police officers, firefighters, and teachers, including survivors, dependents, and beneficiaries who are receiving a federal and/or District benefit.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records and the information in these records may be used:

(1) To disclose pertinent information to the appropriate federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the Department becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

(2) To disclose information to a federal agency, in response to its request in connection with the hiring or retention of an employee, the issuance of a security clearance, the conducting of a suitability or security investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

(3) To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

(4) To disclose information to another federal agency, to a court, or to a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the federal government is a party to the judicial or administrative proceeding. In those cases where the federal government is not a party to the proceeding, records may not be disclosed unless the party complies with the requirements of 31 C.F.R. 1.11.

(5) To disclose information to the National Archives and Records Administration for use in records management inspections and its role as an Archivist.

(6) To disclose information to the Department of Justice when seeking legal advice, or for use in any proceeding, or to prepare for a proceeding, when any of the following is a party to, has an interest in, or is likely to be affected by the proceeding:

(A) The Department or any component thereof;

(B) Any employee of the Department in his or her official capacity;

(C) Any employee of the Department in his or her individual capacity where the Department of Justice or the Department has agreed to represent the employee; or

(D) The federal funds established by the Act to pay benefit payments.

(7) To disclose information to contractors, subcontractors, financial agents, grantees, auditors, actuaries, interns, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Department, including the District.

(8) To disclose information needed to adjudicate a claim for benefit payments or information needed to conduct an analytical study of benefits being paid under such programs as: Social Security Administration's Old Age, Survivor, and Disability Insurance and Medical Programs; military retired pay programs; and federal civilian employee retirement programs (Civil Service Retirement System, Federal Employees Retirement System, and other federal retirement systems).

(9) To disclose to the U.S. Office of Personnel Management (OPM) and to the District, information necessary to verify the election, declination, or waiver of regular and/or optional life insurance coverage, or coordinate with contract carriers the benefit provisions of such coverage.

(10) To disclose to health insurance carriers contracting with OPM to provide a health benefits plan under the federal Employees Health Benefits Program or health insurance carriers contracting with the District to provide a health benefits plan under the health benefits program for District employees, Social Security numbers and other information necessary to identify enrollment in a plan, to verify eligibility for payment of a claim for health benefits, or to carry out the coordination for benefits provisions of such contracts.

(11) To disclose health insurance enrollment information to OPM. OPM provides this enrollment information to their health care carriers who provide a health benefits plan under the Federal Employees Health Benefits Program, or health insurance carriers contracting with the District to provide a health benefits plan under the health benefits program for District employees, Social Security numbers and other information necessary to identify enrollment in a plan, to verify eligibility for payment of a claim for health benefits, or to carry out the coordination for benefits provisions of such contracts.

(12) To disclose to any person possibly entitled to a benefit payment in accordance with the applicable order of precedence or to an executor of a deceased person's estate, information that is contained in the record of a deceased current or former police officer, firefighter, teacher, or judge to assist in properly determining the eligibility and amount of a benefit payment to a surviving recipient, or information that results from such determination.

(13) To disclose to any person who is legally responsible for the care of an individual to whom a record pertains, or who otherwise has an existing, facially-valid power of attorney, including care of an individual who is mentally incompetent or under other legal disability, information necessary to assure application or payment of benefits to which the individual may be entitled.

(14) To disclose to the Parent Locator Service of the Department of Health and Human Services, upon its request, the present address of an individual covered by the system needed for enforcing child support obligations of such individual.

(15) In connection with an examination ordered by the District or the Department under:

(A) Medical examination procedures; or

(B) Involuntary disability retirement procedures to disclose to the representative of an employee, notices, decisions, other written communications, or any other pertinent medical evidence other than medical evidence about which a prudent physician would hesitate to inform the individual; such medical evidence will be disclosed only to a licensed physician, designated in writing for that purpose by the individual or his or her representative. The physician must be capable of explaining the contents of the medical record(s) to the individual and be willing to provide the entire record(s) to the individual.

(16) To disclose information to any source from which the Department seeks additional information that is relevant to a determination of an individual's eligibility for, or entitlement to, coverage under the applicable retirement, life insurance, and health benefits program, to the extent necessary to obtain the information requested.

(17) To disclose information to the Office of Management and Budget at any stage of the legislative coordination and clearance process in connection with private relief legislation as set forth in OMB Circular No. A-19.

(18) To disclose to an agency responsible for the collection of income taxes the information required by an agreement authorized by law to implement voluntary income tax withholdings from benefit payments.

(19) To disclose to the Social Security Administration the names and Social Security numbers of individuals covered by the system when necessary to determine: (1) their vital status as shown in the Social Security Master Records; and (2) whether retirees receiving benefit payments under the District's retirement plan for police officers and firefighters with post-1956 military service credit are eligible for or are receiving old age or survivors benefits under section 202 of the Social Security Act based upon their wages and self-employment income.

(20) To disclose to federal, state, and local government agencies information to help eliminate fraud and abuse in a benefits program administered by a requesting federal, state, or local government agency; to ensure compliance with federal, state, and local government tax obligations by persons receiving benefits payments; and/or to collect debts and overpayments owed to the requesting federal, state, or local government agency.

(21) To disclose to a federal agency, or a person or an organization under contract with a federal agency to render collection services for a federal agency as permitted by law, in response to a written request from the head of the agency or his designee, or from the debt collection contractor, data concerning an individual owing a debt to the federal government.

(22) To disclose, as permitted by law, information to a state court or administrative agency in connection with a garnishment, attachment, or similar proceeding to enforce alimony or a child support obligation.

(23) To disclose information necessary to locate individuals who are owed money or property by a federal, state, or local government agency, or by a financial institution or similar institution, to the government agency owing or otherwise responsible for the money or property (or its agent).

(24) To disclose information necessary in connection with the review of a disputed claim for health benefits to a health plan provider participating in the Federal Employees Health Benefits Program or the health benefits program for employees of the District, and to a program enrollee or covered family member or an enrollee or covered family member's authorized representative.

(25) To disclose information to another federal agency for the purpose of effecting administrative or salary offset against a person employed by that agency, or who is receiving or eligible to receive benefit payments from the agency when the Department as a creditor has

a claim against that person relating to benefit payments.

(26) To disclose information concerning delinquent debts relating to benefit payments to other federal agencies for the purpose of barring delinquent debtors from obtaining federal loans or loan insurance guarantees pursuant to 31 U.S.C. 3720B.

(27) To disclose to state and local governments information used for collecting delinquent debts relating to benefit payments.

(28) To disclose to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(29) To disclose to a former spouse information necessary to explain how his/her former spouse's benefit was computed.

(30) To disclose to a surviving spouse, domestic partner, surviving child, dependent parent, and/or legal guardian information necessary to explain how his/her survivor benefit was computed.

(31) To disclose to a spouse or dependent child (or court-appointed guardian thereof) of an individual covered by the system, upon request, whether the individual (a) changed his/her election from a self-and-family to a self-only health and/or life insurance benefit enrollment,

(b) changed his/her additional survivor benefit election, and/or (c) received a lump-sum refund of his/her retirement contributions.

**Disclosures to consumer reporting agencies:**

Pursuant to 5 U.S.C. 552a(b)(12), disclosures may be made from this system to consumer reporting agencies in accordance with 31 U.S.C. 3711(e).

**Policies and practices for storing, retrieving, safeguarding, retaining and disposing of records in the system:**

**Storage:**

Paper records in this system are stored in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM in secure facilities.

**Retrievability:**

Records may be retrieved by various combinations of name; date of birth; Social Security number; and/or an automatically assigned, system-generated number of the individual to whom they pertain.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a

need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

In accordance with National Archives and Records Administration retention schedule N1-056-09-001 records on a claim for retirement, including salary and service history, survivor annuity elections, and tax and other withholdings are destroyed after 115 years from the date of the former police officer's, firefighter's, teacher's or judge's birth; or 30 years after the date of his/her death, if no application for benefits is received. If a survivor or former spouse receives a benefit payment, such record is destroyed after his/her death. All other records covered by this system may be destroyed in accordance with approved District, federal, and Department guidelines. Paper records are destroyed by shredding or burning. Records in electronic media are electronically erased using accepted techniques.

**System manager(s) and address:**

Director, Office of DC Pensions, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in the system of records, or seeking to contest its contents, should contact the system manager. The system manager will refer the individual to the appropriate point of contact depending on the circumstances of the request. Individuals must furnish the following information for their records to be located and identified:

a. Name, including all former names.

b. Date of birth.

c. Social Security number.

d. Signature.

e. Contact information.

Individuals requesting amendment of their records must also follow the Department's Privacy Act regulations regarding verification of identity and amendment of records (31 CFR part 1 subpart C, appendix A).

**Record access procedures:**

See "Notification procedure," above.

**Contesting record procedures:**

See "Notification procedure," above.

**Record source categories:**

The information in this system is obtained from:

a. The individual to whom the information pertains.

b. District pay, leave, and allowance records.

c. Health benefits and life insurance plan systems records maintained by the Office of Personnel Management, the District, and health and life insurance carriers.

d. Federal civilian retirement systems.

e. Military retired pay system records.

f. Social Security Old Age, Survivor, and Disability Insurance and Medicare Programs.

g. Official personnel folders.

h. The individual's co-workers and supervisors.

i. Physicians who have examined or treated the individual.

j. Surviving spouse, domestic partners, child(ren), former spouse(s), former domestic partner(s), and/or dependent parent(s) of the individual to whom the information pertains.

k. State courts or support enforcement agencies.

l. Credit bureaus and financial institutions.

m. Government Offices of the District of Columbia, including the DC Retirement Board.

n. The General Services Administration National Payroll Center.

o. Educational institutions.

p. Other components of the Department of the Treasury.

q. The Department of Justice.

r. Death reporting sources

**Exemptions claimed for the system:**

None.

**TREASURY/DO .216**

**System name:**

Treasury Security Access Control and Certificates Systems.

**System location:**

Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Treasury employees, contractors, media representatives, other individuals requiring access to Treasury facilities or to receive government property, and those who need to gain access to a Treasury DO cyber asset including the network, LAN, desktops and notebooks.

**Categories of records in the system:**

Individual's application for security/access badge, individual's photograph, fingerprint record, special credentials, allied papers, registers, and logs reflecting sequential numbering of security/access badges. The system also contains information needed to establish accountability and audit control of digital certificates that have been assigned to personnel who require access to Treasury DO cyber assets including the DO network and LAN as well as those who transmit electronic data that requires protection by enabling the use of public key cryptography. It also contains records that are needed to authorize an individual's access to a Treasury network.

Records may include the individual's name, organization, work telephone number, Social Security Number, date of birth, Electronic Identification Number, work e-mail address, username and password, country of birth, citizenship, clearance and status, title, home address and phone number, biometric data including fingerprint minutia, and alias names.

Records on the creation, renewal, replacement or revocation of digital certificates, including evidence provided by applicants for proof of identity and authority, sources used to verify an applicant's identity and authority, and the certificates issued, denied and revoked, including reasons for denial and revocation.

**Authority for maintenance of the system:**

5 U.S.C. 301; 31 U.S.C. 321; the Electronic Signatures in Global and National Commerce Act, Pub. L. 106-229, and E.O. 9397 (SSN).

**Purpose(s):**

The purpose is to: improve security to both Treasury DO physical and cyber assets; maintain records concerning the security/access badges issued; restrict entry to installations and activities; ensure positive identification of personnel authorized access to restricted areas;

maintain accountability for issuance and disposition of security/access badges; maintain an electronic system to facilitate secure, on-line communication between Federal automated systems, between Federal employees or contractors, and/or the public, using digital signature technologies to authenticate and verify identity; provide a means of access to Treasury cyber assets including the DO network, LAN, desktop and laptops; and to provide mechanisms for non-repudiation of personal identification and access to DO sensitive cyber systems including but not limited to human resource, financial, procurement, travel and property systems as well as tax, econometric and other mission critical systems. The system also maintains records relating to the issuance of digital certificates utilizing public key cryptography to employees and contractors for the purpose of transmission of sensitive electronic material that requires protection.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to disclose information to:

(1) Appropriate federal, state, local, and foreign agencies for the purpose of enforcing and investigating administrative, civil or criminal law relating to the hiring or retention of an employee; issuance of a security clearance, license, contract, grant or other benefit;

(2) A court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of or in preparation for civil discovery, litigation, or settlement negotiations, in response to a court order where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) A contractor for the purpose of compiling, organizing, analyzing, programming, or otherwise refining records to accomplish an agency function subject to the same limitations applicable to U.S. Department of the Treasury officers and employees under the Privacy Act;

(4) A Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(5) Third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(6) The Office of Personnel Management, Merit Systems Protection Board, Equal Employment Opportunity Commission, Federal Labor Relations Authority, and the Office of Special Counsel for the purpose of properly administering Federal personnel systems or other agencies' systems in accordance with applicable laws, Executive Orders, and regulations;

(7) Representatives of the National Archives and Records Administration (NARA) who are conducting records management inspections under authority of 44 U.S.C. 2904 and 2906;

(8) Other Federal agencies or entities when the disclosure of the existence of the individual's security clearance is needed for the conduct of government business, and

(9) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist

in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records are stored as electronic media and paper records.

**Retrievability:**

Records may be retrieved by individual's name, social security number, electronic identification number and/or access/security badge number.

**Safeguards:**

Entrance to data centers and support organization offices is restricted to those employees whose work requires them to be there for the system to operate. Identification (ID) cards are verified to ensure that only authorized personnel are present. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols which are periodically changed. Reports produced from the remote printers are in the custody of personnel and financial management officers and are subject to the same privacy controls as other documents of like sensitivity. Access is limited to authorized employees. Paper records are maintained in locked safes and/or file cabinets. Electronic records are password-protected. During non-work hours, records are stored in locked safes and/or cabinets in a locked room.

Protection and control of any sensitive but unclassified (SBU) records are in accordance with TD P 71-10, Department of the Treasury Security Manual. Access to the records is

available only to employees responsible for the management of the system and/or employees of program offices who have a need for such information.

**Retention and disposal:**

In accordance with General Records Schedule 18, records are maintained on government employees and contractor employees for the duration of their employment at the Treasury Department. Records on separated employees are destroyed or sent to the Federal Records Center.

**System manager(s) and address:**

Departmental Offices:

a. Director, Office of Security Programs, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

b. Chief Information Officer, 1750 Pennsylvania Ave., NW, Washington, DC 20006.

**Notification Procedure:**

Individuals seeking notification and access to any record contained in the system of records, or seeking to contest its content, may inquire in accordance with instructions pertaining to individual Treasury components appearing at 31 CFR part 1, subpart C, appendix A.

**Record access procedures:**

See "Notification procedure" above.

**Contesting record procedures:**

See "Notification procedure" above.

**Record source categories:**

The information contained in these records is provided by or verified by the subject individual of the record, supervisors, other personnel documents, and non-Federal sources such as private employers.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .217**

**System name:**

National Financial Literacy Challenge Records--Treasury/DO.

**System location:**

Department of the Treasury, Office of Financial Education, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Individuals covered by the system will be:

- high school students age 13 and older, and
- their teachers who participate in the test.

**Categories of records in the system:**

The system of records will include, for Challenge participants, the high schools' names and addresses; students' names and scores; high school names of award winners; teachers' names, teachers' business email addresses and business phone numbers.

**Authority for maintenance of the system:**

5 U.S.C. 301 and Executive Order 13455.

**Purpose(s):**

The records in this system will be used to identify students whose scores on the Challenge meet the guidelines for award recognition and to distribute the awards to the teachers, who in turn will distribute the awards to the students. Aggregate data and reports related to the program that may be generated and used for analysis will be in a form that is not individually identifiable.

**Routine uses of records maintained in the system including categories of users and purposes of such uses:**

These records may be used to disclose information to:

(1) A court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel or witnesses, for the purpose of civil discovery, litigation, or settlement negotiations or in response to a court order, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(2) A congressional office in response to an inquiry made at the request of the individual (or the individual's parents or guardians) to whom the record pertains;

(3) A contractor or a sponsor, operating in conjunction with the Office of Financial Education to the extent necessary to present appropriate awards;

(4) Appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm, and

(5) These records may be used to disclose award winners to the participant's high school.

**Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Students' scores may be retrieved by name, teacher, and school. Teacher data may be retrieved by name and contact information of the teacher. School information may be retrieved by name and location of the school.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. All official access to the system of records is on a need-to-know basis only, as authorized by the Office of Financial Education of the U.S. Treasury Department. Procedural and physical safeguards, such as personal accountability, audit logs, and specialized communications security, will be used. Each user of computer systems containing records will have individual passwords (as opposed to group passwords) for which the user is responsible. Access to computerized records will be limited, through use of access codes, encryption techniques, and/or other internal mechanisms, to those whose official duties require access.

**Retention and disposal:**

Records will be destroyed at the earliest possible date consistent with applicable records retention policies.

**System manager(s) and address:**

Director of Outreach, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, gain access to records maintained in this system, or seek to contest its content, must submit a written request containing the following elements: (1) identify the record system; (2) identify the category and

type of records sought; and (3) provide at least two items of secondary identification (See 31 CFR part 1, appendix A). Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Records access procedures:**

See "Notification procedure" above.

**Contesting records procedures:**

See "Notification procedure" above.

**Records source categories:**

Student test takers; high school points of contact; and Department of the Treasury records.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .218**

**System Name:**

Making Home Affordable Program--Treasury/DO.

**System location:**

The Office of Financial Stability, Department of the Treasury, Washington, DC. Other facilities that maintain this system of records are located in: Urbana, MD, Dallas, TX, and a backup facility located in Reston, VA, all belonging to the Federal National Mortgage Association (Fannie Mae); in McLean, VA, Herndon, VA, Reston, VA, Richardson, TX, and Denver, CO, facilities operated by or on behalf of the Federal Home Loan Mortgage Corporation (Freddie Mac); and facilities operated by or on behalf of the Bank of New York Mellon (BNYM)

in Nashville, TN, and a backup facility located in Somerset, NJ. Fannie Mae, Freddie Mac and Bank of New York Mellon have been designated as Financial Agents (Financial Agents) for the MHA Program.

**Categories of Individuals Covered By the System:**

This system of records contains information about mortgage borrowers that is submitted to the Department or its Financial Agents by loan servicers that participate in the MHA Program. Information collected pursuant to the MHA Program is subject to the Privacy Act only to the extent that it concerns individuals; information pertaining to corporations and other business entities and organizations is not subject to the Privacy Act.

**Categories of records in the system:**

This system of records contains loan-level information about individual mortgage borrowers (including loan records, financial records, and borrower eligibility records, when appropriate). Typically, these records include, but are not limited to, the individual's name, Social Security Number, mailing address, monthly income, criminal history status as referenced in Section 1481 of the Dodd-Frank statute, the location of the property subject to the loan, property value information, payment history, type of mortgage, and property sale information.

**Authority for maintenance of the system:**

Emergency Economic Stabilization Act of 2008 (Pub. L. 110-343) and Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111-203) (2010).

**Purpose(s):**

The purpose of this system of records is to facilitate administration of the MHA Program by the Department and its Financial Agents, including enabling them to (i) collect and utilize information collected from mortgage loan servicers, including loan-level information about

individual mortgage holders and borrower eligibility; and (ii) produce reports on the performance of the MHA Program, such as reports that concern loan modification eligibility and exception reports that identify certain issues that loan servicers may experience with servicing loans.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies responsible for investigating or prosecuting violations of or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a potential violation of civil or criminal law or regulation;

(2) Disclose information to a federal, state, or local agency, maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a court order where arguably relevant to a proceeding, or in connection with criminal law proceedings;

(4) Provide information to a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(5) Provide information to third parties during the course of a Department investigation as it relates to the MHA Program to the extent necessary to obtain information pertinent to that investigation;

(6) Disclose information to a consumer reporting agency to use in obtaining credit reports;

(7) Disclose information to a debt collection agency for use in debt collection services;

(8) Disclose information to a Financial Agent of the Department, its employees, agents, and contractors, or to a contractor of the Department, for the purpose of assessing the quality of and efficient administration of the MHA Program and compliance with relevant guidelines, agreements, directives and requirements, and subject to the same or equivalent limitations applicable to the Department's officers and employees under the Privacy Act;

(9) Disclose information originating or derived from participating loan servicers back to the same loan servicers as needed, for the purposes of audit, quality control, and reconciliation and response to borrower requests about that same borrower;

(10) Disclose information to Financial Agents, financial institutions, financial custodians, and contractors to: (a) process mortgage loan modification applications, including, but not limited to, enrollment forms; (b) implement, analyze and modify programs relating to the MHA Program; (c) investigate and correct erroneous information submitted to the Department or its Financial Agents; (d) compile and review data and statistics and perform research, modeling and data analysis to improve the quality of services provided under the MHA Program or otherwise improve the efficiency or administration of the MHA Program; or (e) develop, test and enhance computer systems used to administer the MHA Program; with all activities subject to the same or equivalent limitations applicable to the Department's officers and employees under the Privacy Act;

(11) Disclose information to financial institutions, including banks and credit unions, for the purpose of disbursing payments and/or investigating the accuracy of information required to

complete transactions pertaining to the MHA Program and for administrative purposes, such as resolving questions about a transaction;

(12) Disclose information to the appropriate Federal financial regulator or State financial regulator, or to the appropriate Consumer Protection agency, if that agency has jurisdiction over the subject matter of a complaint or inquiry, or the entity that is the subject of the complaint or inquiry;

(13) Disclose information and statistics to the Department of Housing & Urban Development (HUD), the Department of Commerce (Commerce), Federal financial regulators, the U.S. Department of Justice (DOJ), and the Federal Housing Finance Agency to assess the quality and efficiency of services provided under the MHA Program, to ensure compliance with the MHA Program and other laws, and to report on the Program's overall execution and progress;

(14) Disclose information to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(15) Disclose information to the DOJ for its use in providing legal advice to the Department or in representing the Department in a proceeding before a court, adjudicative body, or other administrative body before which the Department is authorized to appear, where the use

of such information by the DOJ is deemed by the Department to be relevant and necessary to the litigation, and such proceeding names as a party of interests:

(a) The Department or any component thereof, including the Office of Financial Stability (OFS);

(b) Any employee of the Department in his or her official capacity;

(c) Any employee of the Department in his or her individual capacity where DOJ has agreed to represent the employee; or

(d) The United States, where the Department determines that litigation is likely to affect the Department or any of its components, including OFS; and

(16) Disclose information to an authorized recipient who has assured the Department or a Financial Agent of the Department in writing that the record will be used solely for research purposes designed to assess the quality of and efficient administration of the MHA Program, subject to the same or equivalent limitations applicable to the Department's officers and employees under the Privacy Act.

**Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:**

**Storage:**

Information contained in the system of records is stored in a transactional database and an operational data store. Information from the system will also be captured in hard-copy form and stored in filing cabinets managed by personnel working on the MHA Program.

**Retrievability:**

Information about individuals may be retrieved from the system by reference including the mortgage borrower's name, Social Security Number, address, criminal history status, or loan number.

**Safeguards:**

Safeguards designed to protect information contained in the system against unauthorized disclosure and access include, but are not limited to: (i) Department and Financial Agent policies and procedures governing privacy, information security, operational risk management, and change management; (ii) requiring Financial Agent employees to adhere to a code of conduct concerning the aforementioned policies and procedures; (iii) conducting background checks on all personnel with access to the system of records; (iv) training relevant personnel on privacy and information security; (v) tracking and reporting incidents of suspected or confirmed breaches of information concerning borrowers; (vi) establishing physical and technical perimeter security safeguards; (vii) using antivirus and intrusion detection software; (viii) performing risk and controls assessments and mitigation, including production readiness reviews; (ix) establishing security event response teams; and (x) establishing technical and physical access controls, such as role-based access management and firewalls. Loan servicers that participate in the MHA Program (i) have agreed in writing that the information they provide to the Department or to its Financial Agents is accurate, and (ii) have submitted a ``click through'' agreement on a Web site requiring the loan servicer to provide accurate information in connection with using the Program Web site. In addition, the Department's Financial Agents will conduct loan servicer compliance reviews to validate data collection controls, procedures, and records.

**Retention and disposal:**

Information is retained in the system on back-up tapes or in hard-copy form for seven years, except to the extent that either (i) the information is subject to a litigation hold or other legal retention obligation, in which case the data is retained as mandated by the relevant legal requirements, or (ii) the Department and its Financial Agents need the information to carry out the Program. Destruction is carried out by degaussing according to industry standards. Hard copy records are shredded and recycled.

**System manager(s) and address:**

Deputy Assistant Secretary, Fiscal Operations and Policy, Department of the Treasury, 1500 Pennsylvania Avenue NW, Washington, DC 20220.

**Notification procedure:**

Individuals wishing to be notified if they are named in this system of records, to gain access to records maintained in this system, or to amend or correct information maintained in this system, must submit a written request to do so in accordance with the procedures set forth in 31 CFR 1.26-.27. Address such requests to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave. NW, Washington, DC 20220.

**Record access procedures:**

See "Notification Procedure" above.

**Contesting record procedure:**

See "Notification Procedure" above.

**Record source categories:**

Information about mortgage borrowers contained in the system of records is obtained from loan servicers who participate in the MHA Program, or developed by the Department and its Financial Agents in connection with the MHA Program. Information is not obtained directly

from individual mortgage borrowers to whom the information pertains.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .219**

**System name:**

TARP Standards for Compensation and Corporate Governance--Executive Compensation Information.

**System location:**

Office of Financial Stability, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

a. Senior Executive Officers or "SEOs.'' SEOs of TARP recipients will be covered by the system. The term "SEO'' means an employee of the TARP recipient who is a "named executive officer,'' as that term is defined by Instruction 1 to Item 402(a)(3) of Regulation S-K of the Federal securities laws. 17 CFR 229.402(a). A TARP recipient that is a "smaller reporting company,'' as that term is defined by Item 10 of Regulation S-K, 17 CFR 229.10, is required to identify SEOs consistent with the immediately preceding sentence. A TARP recipient that is a "smaller reporting company'' must identify at least five SEOs, even if only three named executive officers are provided in the disclosure pursuant to Item 402(m)(2) of Regulation S-K, 17 CFR 229.402(m)(2), provided that no employee must be identified as an SEO if the

employee's total annual compensation does not exceed $100,000 as defined in Item 402(a)(3)(1) of Regulation S-K. 17 CFR 229.402(a)(3)(1).

b. Most highly compensated employees. Most highly compensated employees of TARP recipients will be covered by the system. The term ''most highly compensated employee'' means the employee of the TARP recipient whose annual compensation is determined to be the highest among all employees of the TARP recipient, provided that, for this purpose, a former employee who is no longer employed as of the first day of the relevant fiscal year of the TARP recipient is not a most highly compensated employee unless it is reasonably anticipated that such employee will return to employment with the TARP recipient during such fiscal year.

c. Other employees. Certain other employees of TARP recipients may be covered by the system in the event that the TARP recipient or the employee requests guidance from the Department with respect to the employee's compensation or the Department otherwise provides guidance with respect to the employee's compensation.

**Categories of records in the system:**

The categories of records include, but are not limited to, identifying information such as:

- name(s), employer;
- employee identification number,
- position, and

quantitative and qualitative information with respect to the employee's performance.

The types of records in the system may be:

- Comprehensive compensation data provided by the individual's employer for current and prior years.
- Information relating to compensation plan design and documentation.

- Company performance data relating to compensation plans.

**Authority for maintenance of the system:**

This system of records is authorized by 31 U.S.C. 321 as well as section 111 of the Emergency Economic Stabilization Act of 2008 ("EESA"), as amended by the American Recovery and Reinvestment Act of 2009 ("ARRA"). 12 U.S.C. 5221.

**Purpose(s):**

The Department of the Treasury collects this information from each TARP recipient in connection with the review of compensation payments and compensation structures applicable to SEOs and certain highly compensated employees. Information with respect to certain payments to highly compensated employees will also be reviewed in connection with a determination of whether such payments were inconsistent with the purposes of section 111 of EESA or TARP, or were otherwise contrary to the public interest.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used:

1. To disclose pertinent information to the appropriate federal, state, or local agency responsible for investigating or prosecuting a violation of, or enforcing or implementing, a statute, rule, regulation, or order, where the Department becomes aware of a potential violation of civil or criminal law or regulation, rule, or order.

2. To provide information to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual who is the subject of the record.

3. To disclose information to another federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the Federal Government is a party to the judicial or administrative proceeding. In those cases where the Federal Government is not a party to the proceeding, records may be disclosed if a subpoena has been signed by a court of competent jurisdiction and agency "Touhy" regulations are followed. See 31 CFR 1.8 et seq.

4. To disclose information to the National Archives and Records Administration (NARA) for use in its records management inspections and its role as an archivist.

5. To disclose information to the United States Department of Justice ("DOJ"), for the purpose of representing or providing legal advice to the Department in a proceeding before a court, adjudicative body, or other administrative body before which the Department is authorized to appear, when such proceeding involves:

(A) The Department or any component thereof;

(B) Any employee of the Department in his or her official capacity;

(C) Any employee of the Department in his or her individual capacity where the Department of Justice or the Department has agreed to represent the employee; or

(D) The United States, when the Department determines that litigation is likely to affect the Department or any of its components; and the use of such records by the DOJ is deemed by the DOJ or the Department to be relevant and necessary to the litigation provided that the disclosure is compatible with the purpose for which records were collected.

6. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Department, when necessary to accomplish an agency function related to this system of

records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to Department officers and employees.

7. To appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise that there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

8. In limited circumstances, for the purpose of compiling or otherwise refining records that may be disclosed to the public in the form of summary reports or other analyses provided on a Department Web site.

**Policies and practices for storing, retrieving, safeguarding, retaining and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

These records may be retrieved by various combinations of employer name, individual name, position and/or level of compensation.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. Data in electronic format is encrypted or password protected. Direct access is limited to employees within the Office of Financial Stability whose duties require access. The building where the records are maintained is locked after hours and has a 24-hour security guard. Personnel screening and training are employed to prevent unauthorized disclosure.

**Retention and disposal:**

The records will be maintained indefinitely until a record disposition schedule submitted to the National Archives Records Administration has been approved.

**System manager(s) and address:**

Director, Office of Compliance, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in the system of records, or seeking to contest its contents, should contact the system manager. Individuals must furnish the following information for their records to be located and identified:

a. Name.

b. Employer.

c. Signature.

d. Contact information.

[Individuals requesting amendment of their records must also follow the Department's Privacy Act regulations regarding verification of identity and amendment of records (31 CFR part 1 subpart C, appendix A).]

**Record access procedures:**

See "Notification procedure," above.

**Contesting record procedures:**

See "Notification procedure," above.

**Record source categories:**

The information in this system is obtained from the individual's employer.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .220**

**System name:**

SIGTARP Hotline Database.

**System location:**

Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Complainants who contact the SIGTARP Hotline.

**Categories of records in the system:**

(1) Correspondence received from Hotline complainants; (2) records created of verbal communications with Hotline complainants; and (3) records used to process Hotline complaints, including information included in SIGTARP's other systems of records.

**Authority for maintenance of the system:**

12 U.S.C. 5231, 5 U.S.C. App. 3, and 5 U.S.C. 301.

**Purpose(s):**

This system consists of complaints received by SIGTARP from individuals and their representatives, oversight committees, and others who conduct business with SIGTARP, and information concerning efforts to resolve these complaints; it serves as a record of the complaints and the steps taken to resolve them.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose pertinent information to appropriate Federal, foreign, State, local, Tribal or other public authorities or self-regulatory organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a potential violation of civil or criminal law or regulation;

(2) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil

discovery, litigation, or settlement negotiations, in response to a subpoena, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) Disclose information to another federal agency to (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records;

(5) Disclose information to the Department of Justice when seeking legal advice, or when (a) the agency or (b) any component thereof, or (c) any employee of the agency in his or her official capacity, or (d) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (e) the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation;

(6) Disclose information to the appropriate foreign, State, local, Tribal, or other public authority or self-regulatory organization for the purpose of (a) consulting as to the propriety of access to or amendment or correction of information obtained from that authority or organization, or (b) verifying the identity of an individual who has requested access to or amendment or correction of records;

(7) Disclose information to contractors and other agents who have been engaged by the Department or one of its bureaus to provide products or services associated with the Department's or bureau's responsibility arising under the FOIA/PA;

(8) Disclose information to the National Archives and Records Administration for use in records management inspections;

(9) Disclose information to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(10) Disclose information to any source, either private or governmental, to the extent necessary to elicit information relevant to a SIGTARP audit or investigation;

(11) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing personnel actions or conducting administrative hearings or appeals, or if needed in the performance of other authorized duties;

(12) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger; and

(13) Disclose information to persons engaged in conducting and reviewing internal and external peer reviews of the Office of Inspector General to ensure adequate internal safeguards and management procedures exist within any office that had received law enforcement authorization

or to ensure auditing standards applicable to government audits by the Comptroller General of the United States are applied and followed.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name of the correspondent and/or name of the individual to whom the record applies.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. The records are accessible to SIGTARP personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons.

**Retention and disposal:**

Paper records are maintained and disposed of in accordance with a record disposition schedule 12 approved by the National Archives Records Administration.

**System manager(s) and address:**

Chief Counsel, Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I),

(e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). See 31 CFR 1.36.

**TREASURY/DO .221**

**System name:**

SIGTARP Correspondence Database.

**System location:**

Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

- (1) correspondents; and
- (2) persons upon whose behalf correspondence was initiated.

**Categories of records in the system:**

- (1) correspondence received by SIGTARP and responses generated thereto; and
- (2) records used to respond to incoming correspondence,
- including information included in SIGTARP's other systems of records.

**Authority for maintenance of the system:**

12 U.S.C. 5231, 5 U.S.C. App. 3, and 5 U.S.C. 301.

**Purpose(s):**

This system consists of correspondence received by SIGTARP from individuals and their representatives, oversight committees, and others who conduct business with SIGTARP and the responses thereto; it serves as a record of in-coming correspondence and the steps taken to respond thereto.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose pertinent information to appropriate Federal, foreign, State, local, Tribal or other public authorities or self-regulatory organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(2) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a subpoena, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) Disclose information to another federal agency to (a) permit a decision as to access, amendment or correction of records made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records;

(5) Disclose information to the Department of Justice when seeking legal advice, or when (a) the agency or (b) any component thereof, or (c) any employee of the agency in his or her official capacity, or (d) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (e) the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party

to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation;

(6) Disclose information to the appropriate foreign, State, local, Tribal, or other public authority or self-regulatory organization for the purpose of (a) consulting as to the propriety of access to or amendment or correction of information obtained from that authority or organization, or (b) verifying the identity of an individual who has requested access to or amendment or correction of records;

(7) Disclose information to contractors and other agents who have been engaged by the Department or one of its bureaus to provide products or services associated with the Department's or bureau's responsibility arising under the FOIA/PA;

(8) Disclose information to the National Archives and Records Administration for use in records management inspections;

(9) Disclose information to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(10) Disclose information to any source, either private or governmental, to the extent necessary to elicit information relevant to a SIGTARP audit or investigation;

(11) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing personnel actions or conducting administrative hearings or appeals, or if needed in the performance of other authorized duties;

(12) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger; and

(13) Disclose information to persons engaged in conducting and reviewing internal and external peer reviews of the Office of Inspector General to ensure adequate internal safeguards and management procedures exist within any office that had received law enforcement authorization or to ensure auditing standards applicable to government audits by the Comptroller General of the United States are applied and followed.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name of the correspondent and/or name of the individual to whom the record applies.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. The records are accessible to SIGTARP personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons.

**Retention and disposal:**

Paper records are maintained and disposed of in accordance with a record disposition schedule 12 approved by the National Archives Records Administration.

**System manager(s) and address:**

Chief Counsel, Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). See 31 CFR 1.36.

**TREASURY/DO .222**

**System name:**

SIGTARP Investigative MIS Database.

**System location:**

Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

- subjects or potential subjects of investigative activities;
- witnesses involved in investigative activities.

**Categories of records in the system:**

(1) reports of investigations, which may include, but are not limited to, witness statements, affidavits, transcripts, police reports, photographs, documentation concerning requests and approval for consensual telephone and consensual non-telephone monitoring, the subject's prior criminal record, vehicle maintenance records, medical records, accident reports, insurance policies, police reports, and other exhibits and documents collected during an investigation;

(2) status and disposition information concerning a complaint or investigation including prosecutive action and/or administrative action;

(3) complaints or requests to investigate;

(4) subpoenas and evidence obtained in response to a subpoena;

(5) evidence logs;

(6) pen registers;

(7) correspondence;

(8) records of seized money and/or property;

(9) reports of laboratory examination, photographs, and evidentiary reports;

(10) digital image files of physical evidence;

(11) documents generated for purposes of SIGTARP's undercover activities;

(12) documents pertaining to the identity of confidential informants; and,

(13) other documents collected and/or generated by the Office of Investigations during the course of official duties.

**Authority for maintenance of the system:**

12 U.S.C. 5231, 5 U.S.C. App. 3, and 5 U.S.C. 301.

**Purpose(s):**

The purpose of this system of records is to maintain information relevant to complaints received by SIGTARP and collected as part of investigations conducted by SIGTARP's Office of Investigations.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose pertinent information to appropriate Federal, foreign, State, local, Tribal or other public authorities or self-regulatory organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a potential violation of civil or criminal law or regulation;

(2) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a subpoena, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) Disclose information to another federal agency to (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records;

(5) Disclose information to the Department of Justice when seeking legal advice, or when (a) the agency or (b) any component thereof, or (c) any employee of the agency in his or her official capacity, or (d) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (e) the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation;

(6) Disclose information to the appropriate foreign, State, local, Tribal, or other public authority or self-regulatory organization for the purpose of (a) consulting as to the propriety of access to or amendment or correction of information obtained from that authority or organization, or (b) verifying the identity of an individual who has requested access to or amendment or correction of records;

(7) Disclose information to contractors and other agents who have been engaged by the Department or one of its bureaus to provide products or services associated with the Department's or bureau's responsibility arising under the FOIA/PA;

(8) Disclose information to the National Archives and Records Administration for use in records management inspections;

(9) Disclose information to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the

compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(10) Disclose information to any source, either private or governmental, to the extent necessary to elicit information relevant to a SIGTARP audit or investigation;

(11) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing personnel actions or conducting administrative hearings or appeals, or if needed in the performance of other authorized duties;

(12) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger; and

(13) Disclose information to persons engaged in conducting and reviewing internal and external peer reviews of the Office of Inspector General to ensure adequate internal safeguards and management procedures exist within any office that had received law enforcement authorization or to ensure auditing standards applicable to Government audits by the Comptroller General of the United States are applied and followed.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievabilitiy:**

Records may be retrieved by name, Social Security Number, and/or case number.

**Safeguards:**

The records are accessible to SIGTARP personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons.

**Retention and disposal:**

These records are currently not eligible for disposal. SIGTARP is in the process of requesting approval from the National Archives and Records Administration of records disposition schedules concerning all records in this system of records.

**System manager(s) and address:**

Chief Counsel, Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Chief Counsel, Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

**TREASURY/DO .223System name:**

SIGTARP Investigative Files Database.

**System location:**

Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

Subjects or potential subjects of investigative activities; witnesses involved in investigative activities.

**Categories of records in the system:**

(1) Reports of investigations, which may include, but are not limited to, witness statements, affidavits, transcripts, police reports, photographs, documentation concerning requests and approval for consensual telephone and consensual non-telephone monitoring, the subject's prior criminal record, vehicle maintenance records, medical records, accident reports, insurance policies, police reports, and other exhibits and documents collected during an investigation; (2) status and disposition information concerning a complaint or investigation including prosecutive action and/or administrative action; (3) complaints or requests to investigate; (4) subpoenas and evidence obtained in response to a subpoena; (5) evidence logs; (6) pen registers; (7) correspondence; (8) records of seized money and/or property; (9) reports of laboratory examination, photographs, and evidentiary reports; (10) digital image files of physical evidence; (11) Documents generated for purposes of SIGTARP's undercover activities; (12) documents pertaining to the identity of confidential informants; and, (13) other documents collected and/or generated by the Office of Investigations during the course of official duties.

**Authority for maintenance of the system:**

12 U.S.C. 5231, 5 U.S.C. App. 3, and 5 U.S.C. 301.

**Purpose(s):**

The purpose of this system of records is to maintain information relevant to complaints received by SIGTARP and collected as part of investigations conducted by SIGTARP's Office of Investigations.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose pertinent information to appropriate Federal, foreign, State, local, Tribal or other public authorities or self-regulatory organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a potential violation of civil or criminal law or regulation;

(2) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a subpoena, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) Disclose information to another federal agency to (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records;

(5) Disclose information to the Department of Justice when seeking legal advice, or when (a) the agency or (b) any component thereof, or (c) any employee of the agency in his or her official capacity, or (d) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (e) the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation;

(6) Disclose information to the appropriate foreign, State, local, Tribal, or other public authority or self-regulatory organization for the purpose of (a) consulting as to the propriety of access to or amendment or correction of information obtained from that authority or organization, or (b) verifying the identity of an individual who has requested access to or amendment or correction of records;

(7) Disclose information to contractors and other agents who have been engaged by the Department or one of its bureaus to provide products or services associated with the Department's or bureau's responsibility arising under the FOIA/PA;

(8) Disclose information to the National Archives and Records Administration for use in records management inspections;

(9) Disclose information to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(10) Disclose information to any source, either private or governmental, to the extent necessary to elicit information relevant to a SIGTARP audit or investigation;

(11) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing personnel actions or

conducting administrative hearings or appeals, or if needed in the performance of other authorized duties;

(12) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger; and

(13) Disclose information to persons engaged in conducting and reviewing internal and external peer reviews of the Office of Inspector General to ensure adequate internal safeguards and management procedures exist within any office that had received law enforcement authorization or to ensure auditing standards applicable to Government audits by the Comptroller General of the United States are applied and followed.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name, Social Security Number, and/or case number.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is stored. The records are accessible to SIGTARP personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons.

**Retention and disposal:**

These records are currently not eligible for disposal. SIGTARP is in the process of requesting approval from the National Archives and Records Administration of records disposition schedules concerning all records in this system of records.

**System manager(s) and address:**

Chief Counsel, Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

**TREASURY/DO .224**

**SYSTEM NAME:**

SIGTARP Audit Files Database.

**System location:**

Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

- auditors,
- certain administrative support staff,

- contractors of SIGTARP, and
- certain subjects and/or witnesses referenced in SIGTARP's audit activities.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

(1) audit reports; and

(2) working papers, which may include copies of correspondence, evidence, subpoenas, other documents collected and/or generated by the Office of Audit during the course of official duties.

**Authority for maintenance of the system:**

12 U.S.C. 5231, 5 U.S.C. App. 3, and 5 U.S.C. 301.

**Purposes:**

This system is maintained in order to act as a management information system for SIGTARP audit projects and personnel and to assist in the accurate and timely conduct of audits.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to:

(1) Disclose pertinent information to appropriate Federal, foreign, State, local, Tribal or other public authorities or self-regulatory organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a potential violation of civil or criminal law or regulation;

(2) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil

discovery, litigation, or settlement negotiations, in response to a subpoena where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) Disclose information to another federal agency to (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records;

(5) Disclose information to the Department of Justice when seeking legal advice, or when (a) the agency or (b) any component thereof, or (c) any employee of the agency in his or her official capacity, or (d) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (e) the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation;

(6) Disclose information to the appropriate foreign, State, local, Tribal, or other public authority or self-regulatory organization for the purpose of (a) consulting as to the propriety of access to or amendment or correction of information obtained from that authority or organization, or (b) verifying the identity of an individual who has requested access to or amendment or correction of records;

(7) Disclose information to contractors and other agents who have been engaged by the Department or one of its bureaus to provide products or services associated with the Department's or bureau's responsibility arising under the FOIA/PA;

(8) Disclose information to the National Archives and Records Administration for use in records management inspections;

(9) Disclose information to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(10) Disclose information to any source, either private or governmental, to the extent necessary to elicit information relevant to a SIGTARP audit or investigation;

(11) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing personnel actions or conducting administrative hearings or appeals, or if needed in the performance of other authorized duties;

(12) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger; and

(13) Disclose information to persons engaged in conducting and reviewing internal and external peer reviews of the Office of Inspector General to ensure adequate internal safeguards and management procedures exist within any office that had received law enforcement authorization

or to ensure auditing standards applicable to Government audits by the Comptroller General of the United States are applied and followed.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by name of the auditor, support staff, contractors, or subject of the audit.

**Safeguards:**

The records are accessible to SIGTARP personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

These records are currently not eligible for disposal. SIGTARP is in the process of requesting approval from the National Archives and Records Administration of records disposition schedules concerning all records in this system of records.

**System manager(s) and address:**

Chief Counsel, Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), 1801 L Street, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). See 31 CFR 1.36.

**TREASURY/DO .225**

**System name:**

TARP Fraud Investigation Information System.

**System location:**

Office of Financial Stability, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Categories of individuals covered by the system:**

The TARP Fraud Investigation Information System contains information about:

(a) Individuals that seek, receive or are entrusted with TARP funds;

(b) Individuals that are:

1. Known perpetrators or suspected perpetrators of a known or possible fraud committed or attempted against TARP programs;

2. Directors, officers, partners, proprietors, employees, and agents, of a business entity;

3. Named as possible witnesses;

4. Actual or potential victims of fraud, including but not limited to mortgage fraud; and

5. Individuals or entities who have applied to any of the TARP programs, recipients of TARP program funds and/or benefits, OFS contractors, OFS agents; or

6. Individuals or entities who have or might have information about reported matters.

**Categories of records in the system:**

This system of records contains information on individuals or entities who seek, receive or are entrusted with TARP funds, are the subject of an investigation or in connection with an investigation, undertaken by OFS into allegations of actual or suspected TARP program fraud, waste, and/or abuse. Typically, these records include, but are not limited to, the individual's name, date of birth, Social Security Number, telephone number(s), residential address(es), e-mail or web address(es), driver's license number, vehicle ownership records, prior criminal history, and other exhibits and documents collected during an investigation.

**Authority for maintenance of the system:**

12 U.S.C. 5211 and 18 U.S.C. 1031.

**Purpose(s):**

The purpose of this system of records is to maintain a database of investigative materials consisting of complaints, inquiries, and investigative referrals pertaining to alleged fraud, waste, and/or abuse committed or alleged to have been committed by third parties against the TARP programs, and of background inquiries conducted on individuals seeking, receiving or entrusted with TARP funds. Information in the system will allow investigators to determine whether to refer matters to the appropriate authority for further investigation and possible criminal, civil, or administrative action.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used:

1. To disclose pertinent information to appropriate Federal, foreign, State, local, Tribal or other public authorities or self-regulatory organizations responsible for investigating or prosecuting

the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a potential violation of civil or criminal law or regulation.

2. Provide information to a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains.

3. Disclose information to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the Federal Government is a party to the judicial or administrative proceeding. In those cases where the Federal Government is not a party to the proceeding, records may be disclosed if a subpoena has been signed by a court of competent jurisdiction and agency "Touhy" regulations are followed. See 31 CFR 1.8 et seq.

4. To disclose information to the National Archives and Records Administration (NARA) for use in its records management inspections and its role as an Archivist.

5. To disclose information to the United States Department of Justice (DOJ), for the purpose of representing or providing legal advice to the Department of the Treasury (Department) in a proceeding before a court, adjudicative body, or other administrative body before which the Department is authorized to appear, when such proceeding involves:

(a) The Department or any component thereof;

(b) Any employee of the Department in his or her official capacity;

(c) Any employee of the Department in his or her individual capacity where the DOJ or the Department has agreed to represent the employee; or

(d) The United States, when the Department determines that litigation is likely to affect the Department or any of its components; and the use of such records by the DOJ is deemed by the DOJ or the Department to be relevant and necessary to the litigation

provided that the disclosure is compatible with the purpose for which records were collected.

6. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Department, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to Department officers and employees.

7. To appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise that there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

8. To disclose information to the appropriate Federal, foreign, State, local, Tribal, or other public authority or self-regulatory organization for the purpose of consulting as to the propriety of access to or amendment or correction of information obtained from that authority or organization, or verifying the identity of an individual who has requested access to or amendment or correction of records.

**Policies and practices for storing, retrieving, safeguarding, retaining and disposing of records in the system:**

**Storage:**

These records are maintained in both an electronic media and paper records.

**Retrievability:**

These records may be retrieved by various combinations of employer name and or individual name.

**Safeguards:**

Where feasible, data in electronic format is encrypted or password protected. Access to data and records is limited to only those employees within the Office of Financial Stability whose duties require access. Physical records are kept securely locked at a controlled, limited-access facility. Personnel screening and training are employed to prevent unauthorized disclosure.

**Retention and disposal:**

The records will be maintained indefinitely until a record disposition schedule submitted to the National Archives Records Administration has been approved.

**System manager(s) and address:**

Supervisory Fraud Specialist, Office of Financial Stability, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions

appearing at 31 CFR part 1, subpart C, appendix A. Address inquiries to: Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(k)(2).

**Record access procedure:**

See "Notification Procedure" above.

**Contesting record procedure:**

See "Notification Procedure" above.

**Record source categories:**

Information contained in this system is obtained from mortgage servicers, other government agencies or self-regulatory organizations, Treasury's financial agents, commercial databases, and/or witnesses or other third parties having information relevant to an investigation. Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(k)(2).

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), (I) and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2).

**TREASURY/DO .226**

**System Name:**

Validating EITC Eligibility with State Data Pilot Project Records –Treasury/DO.

**System location:**

Office of the Fiscal Assistant Secretary, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC.

**Categories of individuals covered by the system:**

Individuals who file for State-administered public assistance benefits in States participating in the Department's pilot program.

**Categories of records in the system:**

These records include information pertaining to the Department of the Treasury's pilot project "Assessing State Data for Validating EITC Eligibility." Records include, but are not limited to, the application[s] for State-administered benefits, including subsequent recertification documentation and other documents supporting eligibility for State-administered benefit programs. The records may contain taxpayer names, Taxpayer Identification Numbers, Social Security Numbers, and other representative authorization information.

**Authority for maintenance of the system:**

The Consolidated Appropriations Act, 2010 (Pub. L. 111–117, 123 Stat. 3034, 3171–3172); 5 U.S.C. 301; 31 U.S.C. 321.

**Purpose:**

The purpose of this system is to determine whether data maintained by up to five States in their public assistance and other databases can assist in identifying both ineligible individuals who receive improper Earned Income Tax Credit payments and eligible individuals who are not claiming the EITC.

**Routine uses of records maintained in the system including categories of users and purposes of such uses:**

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the Department determines that the purpose of the disclosure is compatible with the purpose for which the Department collected the records, and no privilege is asserted.

(1) Disclose to the appropriate State agencies responsible for validating results of the data matching initiative with specific individual case file research.

(2) Provide information to a Congressional Office in response to an inquiry made at the request of the individual to whom the records pertain.

(3) Disclose information to a contractor, including a consultant hired by Treasury, to the extent necessary for the performance of a contract.

**(**4) To appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(5) Disclose information to the National Archives and Records Administration (“NARA”) for use in its records management inspections and its role as an Archivist.

**Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records in the System:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

By taxpayer name and Taxpayer Identification Number, Social Security Number, employer identification number, or similar number assigned by the IRS.

**Safeguards:**

Access to electronic records is restricted to authorized personnel who have been issued non-transferrable access codes and passwords. Other records are maintained in locked file cabinets or rooms with access limited to those personnel whose official duties require access. The facilities have 24-hour on-site security.

**Retention and disposal:**

Electronic and paper records will be maintained indefinitely until a records disposition schedule is approved by the National Archives and Records Administration.

**System manager(s) and address:**

Deputy Assistant Secretary for Fiscal Operations and Policy, Office of the Fiscal Assistant Secretary, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Notification procedure:**

Individuals seeking to determine if this system of records contains a record pertaining to themselves may inquire in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Inquiries should be addressed as in "Record Access Procedures" below.

**Records access procedures:**

Individuals seeking access to any record contained in this system of records, or seeking to contest its content, may inquire in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Inquiries should be addressed to Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave., NW, Washington, DC 20220.

**Contesting records procedures:**

26 U.S.C. 7852(e) prohibits Privacy Act amendment of tax records. For all other records, see "Records Access Procedures" above.

**Records source categories:**

Records in this system are provided by the States' department for public assistance and health services, and/or the departments of revenue for the States participating in the pilot project.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .301**

**System name:**

TIGTA General Personnel and Payroll.

**System location:**

National Headquarters, 1401 H Street, NW, Washington, DC 20005, field offices listed in Appendices A and B, Bureau of Public Debt, 200 Third Street, Parkersburg, WV 26106-1328, and Transaction Processing Center, U.S. Department of Agriculture, National Finance Center.

**Categories of individuals covered by the system:**

Current and former TIGTA employees.

**Categories of records in the system:**

This system consists of a variety of records relating to personnel actions and determinations made about TIGTA employees. These records contain data on individuals required by the Office of Personnel Management (OPM) and which may also be contained in the Official Personnel Folder (OPF). This system may also contain letters of commendation, recommendations for awards, awards, reprimands, adverse or disciplinary charges, and other records which OPM and TIGTA require or permit to be maintained. This system may include records that are maintained in support of a personnel action such as a position management or position classification action, a reduction-in-force action, and priority placement actions. Other records maintained about an individual in this system are performance appraisals and related records, expectation and payout records, employee performance file records, suggestion files, award files, financial and tax records, back pay files, jury duty records, outside employment statements, clearance upon separation documents, unemployment compensation records, adverse and disciplinary action files, supervisory drop files, records relating to personnel actions, furlough and recall records, work measurement records, emergency notification records, and employee locator and current address records. This system includes records created and maintained for purposes of administering the payroll system. Time-reporting records include timesheets and records indicating the number of hours by TIGTA employee attributable to a

particular project, task, or audit. This system also includes records related to travel expenses and/or costs. This system includes records concerning employee participation in the Telecommuting program. This system also contains records relating to life and health insurance, retirement coverage, designations of beneficiaries, and claims for survivor or death benefits.

**Authority for maintenance of the system:**

5 U.S.C. app. 3, and 5 U.S.C. 301, 1302, 2951, 4506, Ch. 83, 87, and 89.

**Purpose(s):**

This system consists of records compiled for personnel, payroll and time-reporting purposes. In addition, this system contains all records created and/or maintained about employees as required by the Office of Personnel Management (OPM) as well as documents relating to personnel matters and determinations. Retirement, life, and health insurance benefit records are collected and maintained in order to administer the Federal Employee's Retirement System (FERS), Civil Service Retirement System (CSRS), Federal Employee's Group Life Insurance Plan, and, the Federal Employees' Health Benefit Program.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosures of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal, or other relevant enforcement information or other pertinent information that has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear when: (a) The agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party of the litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties in order to obtain information pertinent and necessary for the hiring or retention of an individual and/or to obtain information pertinent to an investigation;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(10) Provide information to educational institutions for recruitment and cooperative education purposes;

(11) Provide information to a federal, state, or local agency so that the agency may adjudicate an individual's eligibility for a benefit;

(12) Provide information to a federal, state, or local agency or to a financial institution as required by law for payroll purposes;

(13) Provide information to federal agencies to effect inter-agency salary offset and administrative offset;

(14) Provide information to a debt collection agency for debt collection services;

(15) Respond to state and local authorities for support garnishment interrogatories;

(16) Provide information to private creditors for the purpose of garnishment of wages of an employee if a debt has been reduced to a judgment;

(17) Provide information to a prospective employer of a current or former TIGTA employee;

(18) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger;

(19) Provide information to the Office of Workers' Compensation,

Veterans Administration Pension Benefits Program, Social Security (Old Age, Survivor and Disability Insurance) and Medicare Programs, Federal civilian employee retirement systems, and other Federal agencies when requested by that program, for use in determining an individual's claim for benefits;

(20) Provide information necessary to support a claim for health insurance benefits under the Federal Employees' Health Benefits Program to a health insurance carrier or plan participating in the program;

(21) Provide information to hospitals and similar institutions to verify an employee's coverage in the Federal Employees' Health Benefits Program;

(22) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(23) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Disclosure to consumer reporting agencies:**

Disclosures pursuant to 5 U.S.C. 552a(b)(12). Disclosures of debt information concerning a claim against an individual may be made from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Electronic media, paper records, and microfiche.

**Retrievability:**

Name, Social Security Number, and/or claim number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Records are maintained and disposed of in accordance with the appropriate National Archives and Records Administration General Records Schedule, Nos. 1 and 2.

**System manager(s) and address:**

General Personnel Records--Associate Inspector General for Mission Support/Chief Financial Officer. Time-reporting records: (1) For Office of Audit employees--Deputy Inspector General for Audit; (2) For Office of Chief Counsel employees--Chief Counsel; (3) For Office of Investigations employees--Deputy Inspector General for Investigations; (4) For Office of Inspections and Evaluations employees--Deputy Inspector General for Inspections and Evaluations; (5) For Office of Information Technology employees--Chief Information Officer; and (6) For Office of Mission Support/Chief Financial Officer employees—Associate Inspector General for Mission Support/Chief Financial Officer--1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005.

**Record access procedures:**

See “Notification Procedures” above.

**Contesting record procedures:**

See “Notification Procedures” above.

**Record source categories:**

Information in this system of records either comes from the individual to whom it applies, is derived from information supplied by that individual, or is provided by Department of the Treasury and other federal agency personnel and records.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .302**

**System name:**

TIGTA Medical Records.

**System location:**

(1) Health Improvement Plan Records--Office of Investigations, 1401 H Street, NW, Washington, DC 20005 and field division offices listed in Appendix A; and, (2) All other records of: (a) Applicants and current TIGTA employees: Office of Mission Support/Chief Financial Officer, TIGTA, 1401 H Street, NW, Washington, DC 20005 and/or Bureau of Public Debt, 200 Third Street, Parkersburg, WV 26106-1328; and, (b) former TIGTA employees: National Personnel Records Center, 9700 Page Boulevard, St. Louis, MO 63132.

**Categories of individuals covered by the system:**

(1) Applicants for TIGTA employment; (2) Current and former TIGTA employees; (3) Applicants for disability retirement; and, (4) Visitors to TIGTA offices who require medical attention while on the premises.

**Categories of records in the system:**

(1) Documents relating to an applicant's mental/physical ability to perform the duties of a position; (2) Information relating to an applicant's rejection for a position because of medical reasons; (3) Documents relating to a current or former TIGTA employee's mental/physical ability to perform the duties of the employee's position; (4) Disability retirement records; (5) Health history questionnaires, medical records, and other similar information for employees participating in the Health Improvement Program; (6) Fitness-for-duty examination reports; (7) Employee assistance records; (8) Injury compensation records relating to on-the-job injuries of current or former TIGTA employees; and, (9) Records relating to the drug testing program.

**Authority for maintenance of the system:**

5 U.S.C. app. 3, 5 U.S.C. 301, 3301, 7301, 7901, and Ch. 81, 87 and 89.

**Purpose(s):**

To maintain records related to employee physical exams, fitness-for-duty evaluations, drug testing, disability retirement claims, participation in the Health Improvement Program, and worker's compensation claims. In addition, these records may be used for purposes of making suitability and fitness-for duty determinations.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

With the exception of Routine Use "(1)," none of the other Routine Uses identified for this system of records are applicable to records relating to drug testing under Executive Order 12564 "Drug-Free Federal Work Place." Further, such records shall be disclosed only to a very limited number of officials within the agency, generally only to the agency Medical Review Official (MRO), the administrator of the agency Employee Assistance Program, and the management official empowered to recommend or take adverse action affecting the individual.

Records may be used to:

(1) Disclose the results of a drug test of a Federal employee pursuant to an order of a court of competent jurisdiction where required by the United States Government to defend against any challenge against any adverse personnel action;

(2) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(3) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(4) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear when (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(5) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil

discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(6) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(7) Provide information to third parties in order to obtain information pertinent and necessary for the hiring or retention of an individual and/or to obtain information pertinent to an investigation;

(8) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(9) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(10) Provide information to Federal or State agencies responsible for administering Federal benefits programs and private contractors engaged in providing benefits under Federal contracts;

(11) Disclose information to an individual's private physician where medical considerations or the content of medical records indicate that such release is appropriate;

(12) Disclose information to other Federal or State agencies to the extent provided by law or regulation;

(13) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger;

(14) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the

Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(15) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Paper records, electronic media, and x-rays.

**Retrievability:**

Records are retrievable by name, Social Security Number, date of birth and/or claim number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Records are maintained and disposed of in accordance with the appropriate National Archives and Records Administration General Records Schedule, No. 1.

**System manager(s) and address:**

(1) Health Improvement Program records--Deputy Inspector General for Investigations, TIGTA, 1401 H Street, NW, Washington, DC 20005; and, (2) All other records--Associate Inspector General for Mission Support/Chief Financial Officer, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart c, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Section, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005.

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

(1) The subject of the record; (2) Medical personnel and institutions; (3) Office of Workers' Compensation personnel and records; (4) Military Retired Pay Systems Records; (5)

Federal civilian retirement systems; (6) General Accounting Office pay, leave allowance cards; (7) OPM Retirement, Life Insurance and Health Benefits Records System and Personnel Management Records System; (8) Department of Labor; and, (9) Federal Occupation Health Agency.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .303**

**System name:**

TIGTA General Correspondence.

**System location:**

National Headquarters, 1401 H Street, NW, Washington, DC 20005, and field offices listed in Appendices A and B.

**Categories of individuals covered by the system:**

(1) Initiators of correspondence; and, (2) Persons upon whose behalf the correspondence was initiated.

**Categories of records in the system:**

(1) Correspondence received by TIGTA and responses generated thereto; and, (2) Records used to respond to incoming correspondence. Special Categories of correspondence may be included in other systems of records described by specific notices.

**Authority for maintenance of the system:**

5 U.S.C. app. 3 and 5 U.S.C. 301.

**Purpose(s):**

This system consists of correspondence received by TIGTA from individuals and their representatives, oversight committees, and others who conduct business with TIGTA and the responses thereto; it serves as a record of in-coming correspondence and the steps taken to respond thereto.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosures of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records

by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in connection with criminal law proceedings or in response to a subpoena where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(7) Provide information to the news media, in accordance with guidelines contained in 28 CFR 50.2;

(8) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(9) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(10) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained

by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Paper records and electronic media.

**Retrievability:**

By name of the correspondent and/or name of the individual to whom the record applies.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Paper records are maintained and disposed of in accordance with a record disposition schedule approved by the National Archives Records Administration. TIGTA is in the process of requesting approval for a record retention schedule for electronic records maintained in this system. These electronic records will not be destroyed until TIGTA receives such approval.

**System manager(s) and address:**

Associate Inspector General for Mission Support/Chief Financial Officer, TIGTA, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2). Non-exempt sources of information include: (1) Initiators of the correspondence; and (2) Federal Treasury personnel and records.

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). See 31 CFR 1.36.

**TREASURY/DO .304**

**System name:**

TIGTA General Training Records.

**System location:**

National Headquarters, 1401 H Street, NW, Washington, DC 20005; Federal Law Enforcement Training Center (FLETC), Glynco, GA 31524.

**Categories of individuals covered by the system:**

(1) TIGTA employees; and, (2) Other Federal or non-Government individuals who have participated in or assisted with training programs as instructors, course developers, or interpreters.

**Categories of records in the system:**

(1) Course rosters; (2) Student registration forms; (3) Nomination forms; (4) Course evaluations; (5) Instructor lists; (6) Individual Development Plans (IDPs); (7) Counseling records; (8) Examination and testing materials; (9) Payment records; (10) Continuing professional education requirements; (11) Officer safety files and firearm qualification records; and, (12) Other training records necessary for reporting and evaluative purposes.

**Authority for maintenance of the system:**

5 U.S.C. app. 3, 5 U.S.C. 301 and Ch. 41, and Executive Order 11348, as amended by Executive Order 12107.

**Purpose(s):**

These records are collected and maintained to document training received by TIGTA employees.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Records may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records

by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties to the extent necessary to obtain information pertinent to the training request or requirements and/or in the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(10) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(11) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Paper and electronic media.

**Retrievability:**

Name, Social Security Number, course title, date of training, and/or location of training.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Records are maintained and disposed in accordance with the appropriate National Archives and Records Administration General Records Schedule, No. 1.

**System manager(s) and address:**

(1) For records concerning Office of Investigations employees--Deputy Inspector General for Investigations; (2) For records concerning Office of Audit employees--Deputy Inspector General for Audit; (3) For Office of Chief Counsel employees--Chief Counsel; and, (4) For Office of Inspections and Evaluations—Deputy Inspector General for Inspections and Evaluations; (5) For Office of Information Technology employees—Chief Information Officer; and, (6) For Office of Mission Support/Chief Financial Officer employees—Associate Inspector General for Mission Support/Chief Financial Officer—1401 H Street, NW, Washington, DC, 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005.

**Record access procedures:**

See “Notification Procedures” above.

**Contesting record procedures:**

See “Notification Procedures” above.

**Record source categories:**

(1) The subject of the record; and, (2) Treasury personnel and records.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .305**

**System name:**

TIGTA Personal Property Management Records.

**System location:**

TIGTA, 4800 Buford Hwy, Chamblee, GA 30341.

**Categories of individuals covered by the system:**

Current and former TIGTA employees.

**Categories of records in the system:**

Information concerning personal property assigned to TIGTA employees including descriptions and identifying information about the property, maintenance records, and other similar records.

**Authority for maintenance of the system:**

5 U.S.C. app. 3, 5 U.S.C. 301, and 41 CFR Subtitle C Ch. 101 and 102.

**Purpose(s):**

The purpose of this system is to maintain records concerning personal property, including but not limited to, laptop and desktop computers and other Information Technology and related accessories, fixed assets, , motor vehicles, firearms and other law enforcement equipment, and communications equipment, for use in official duties.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Records may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information that has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when: (a) The agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(10) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(11) To appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether

maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Electronic media.

**Retrievability:**

Indexed by name and/or identification number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Archived paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Records are maintained and disposed of in accordance with the appropriate National Archives and Records Administration General Records Schedules, Nos. 4 and 10.

**System manager(s) and address:**

Deputy Inspector General for Mission Support/Chief Financial Officer, Office of Mission Support/Chief Financial Officer, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005.

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

(1) The subject of the record; (2) Treasury personnel and records; (3) Vehicle maintenance facilities; (4) Property manufacturer; and, (5) Vehicle registration and licensing agencies.

**Exemptions claimed for the system:**

None.

**TREASURY/DO .306**

**System name:**

TIGTA Recruiting and Placement Records.

**System location:**

Office of Mission Support/Chief Financial Officer, NW1401 H Street, NW, Washington, DC 20005 and/or Bureau of Public Debt, 200 Third Street, Parkersburg, WV 26106-1328.

**Categories of individuals covered by the system:**

(1) Applicants for employment; and, (2) Current and former TIGTA employees.

**Categories of records in the system:**

(1) Application packages and Resumes; (2) Related correspondence; and, (3) Documents generated as part of the recruitment and hiring process.

**Authority for maintenance of the system:**

5 U.S.C. app. 3, 5 U.S.C. 301 and Ch. 33, and Executive Orders 10577 and 11103.

**Purpose(s):**

The purpose of this system is to maintain records received from applicants applying for positions with TIGTA and relating to determining eligibility for employment.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when: (a) The agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties to the extent necessary to obtain information pertinent to the recruitment, hiring, and/or placement determination and/or during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions

or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(10) Disclose information to officials of Federal agencies for purposes of consideration for placement, transfer, reassignment, and/or promotion of TIGTA employees;

(11) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(12) To appropriate agencies, entities, and persons when: (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Paper and electronic media.

**Retrievability:**

Records are indexed by name, Social Security Number, and/or vacancy announcement number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access disposal.

**Retention and disposal:**

Records in this system are maintained and disposed of in accordance with the appropriate National Archives and Records Administration General Records Schedule, No. 1.

**System manager(s) and address:**

Associate Inspector General for Mission Support/Chief Financial Officer, NW1401 H Street NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(k)(5) and (k)(6).

**Record access procedures:**

See “Notification Procedures” above.

**Contesting record procedures:**

See “Notification Procedures” above.

**Record source categories:**

(1) The subject of the record; (2) Office of Personnel Management; and, (3) Treasury personnel and records.

**Exemptions claimed for the system:**

Some records in this system have been designated as exempt from 5 U.S.C. 552a (c)(3), (d)(1), (2), (3), and (4), (e)(1), (e)(4)(G), (H), and (I), and (f) pursuant to 5 U.S.C. 552a (k)(5) and (k)(6). See 31 CFR 1.36.

**TREASURY/DO .307**

**System name:**

TIGTA Employee Relations Matters, Appeals, Grievances, and Complaint Files.

**System location:**

Office of Mission Support/Chief Financial Officer, TIGTA, 1401 H Street, NW, Washington, DC 20005.

**Categories of individuals covered by the system:**

Current, former, and prospective TIGTA employees.

**Categories of records in the system:**

(1) Requests, (2) Appeals, (3) Complaints, (4) Letters or notices to the subject of the record, (5) Records of hearings, (6) Materials relied upon in making any decision or

determination, (7) Affidavits or statements, (8) Investigative reports, and, (9) Documents effectuating any decisions or determinations.

**Authority for maintenance of the system:**

5 U.S.C. app 3 and 5 U.S.C. 301, Ch. 13, 31, 33, 73, and 75.

**Purpose(s):**

This system consists of records compiled for administrative purposes concerning personnel matters affecting current, former, and/or prospective TIGTA employees.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or

her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Provide information to Executive agencies, including, but not limited to the Office of Personnel Management, Office of Government Ethics, and General Accounting Office in order to obtain legal and/or policy guidance;

(10) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions

or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(11) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(12) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Paper and electronic media.

**Retrievability:**

Indexed by the name of the individual and case number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subjects of a background investigation, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Records are maintained and disposed of in accordance with the appropriate National Archives and Records Administration General Records Schedule, No. 1.

**System manager(s) and address:**

Associate Inspector General for Mission Support/Chief Financial Officer, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

(1) The subject of the records; (2) Treasury personnel and records; (3) Witnesses; (4) Documents relating to the appeal, grievance, or complaint; and, (5) EEOC, MSPB, and other similar organizations.

**Exemptions claimed for the system:**

This system may contain investigative records that are exempt from 5 U.S.C. 552a(c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(See 31 CFR 1.36.)

**TREASURY/DO .308**

**System name:**

TIGTA Data Extracts.

**System location:**

National Headquarters, 1401 H Street, NW, Washington, DC 20005, Office of Mission Support/Chief Financial Officer, 4800 Buford Highway, Chamblee, GA 30341, and Office of Investigations, Strategic Enforcement Division, 550 Main Street, Cincinnati, OH 45202.

**Categories of individuals covered by the system:**

(1) The subjects or potential subjects of investigations; (2) Individuals who have filed, are required to file tax returns, or are included on tax returns, forms, or other information filings; (3)

Entities who have filed or are required to file tax returns, IRS forms, or information filings as well as any individuals listed on the returns, forms and filings; and, (4) Taxpayer representatives.

**Categories of records in the system:**

Data extracts from various databases maintained by the Internal Revenue Service consisting of records collected in performance of its tax administration responsibilities as well as records maintained by other governmental agencies, entities, and public record sources. This system also contains information obtained via TIGTA's program of computer matches.

**Authority for maintenance of the system:**

5 U.S.C. app. 3 and 5 U.S.C. 301.

**Purpose(s):**

This system consists of data extracts from various electronic systems of records maintained by governmental agencies and other entities. The data extracts generated by TIGTA are used for audit and investigative purposes and are necessary to identify and deter fraud, waste, and abuse in the programs and operations of the Internal Revenue Service (IRS) and related entities as well as to promote economy, efficiency, and integrity in the administration of the internal revenue laws and detect and deter wrongdoing by IRS and TIGTA employees.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information that has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(10) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(11) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Paper records and electronic media.

**Retrievability:**

By name, Social Security Number, Taxpayer Identification Number, and/or employee identification number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

TIGTA is in the process of requesting approval of a new record retention schedule concerning the records in this system of records. These records will not be destroyed until TIGTA receives approval from the National Archives and Records Administration.

**System manager(s) and address:**

Associate Inspector General for Mission Support/Chief Financial Officer, TIGTA, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Washington, DC 20005. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above. 26 U.S.C. 7852(e) prohibits Privacy Act amendment of tax records.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2). Non-exempt record source categories include the following: Department of the Treasury personnel and records.

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a(c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). (See 31 CFR 1.36.)

**TREASURY/DO .309**

**System name:**

TIGTA Chief Counsel Case Files.

**System location:**

Office of Chief Counsel, 1401 H Street, NW, Washington, DC 20005.

**Categories of individuals:**

Parties to and persons involved in litigations, actions, personnel matters, administrative claims, administrative appeals, complaints, grievances, advisories, and other matters assigned to, or under the jurisdiction of, the Office of Chief Counsel.

**Categories of records in the system:**

(1) Memoranda, (2) Complaints, (3) Claim forms, (4) Reports of Investigations, (5) Accident reports, (6) Witness statements and affidavits, (7) Pleadings, (8) Correspondence, (9) Administrative files, (10) Case management documents, and (11) Other records collected or generated in response to matters assigned to the Office of Chief Counsel.

**Purpose(s):**

This system contains records created and maintained by the Office of Chief Counsel for purposes of providing legal and programmatic service to TIGTA.

**Authority for maintenance of the system:**

5 U.S.C. app. 3, and 5 U.S.C. 301.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing, or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information that has requested information relevant to, or necessary to, the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purposes of litigating an action or seeking legal advice;

(6) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to an investigation or matter under consideration;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Provide information to Executive agencies, including, but not limited to the Office of Personnel Management, Office of Government Ethics, and General Accounting Office;

(10) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties;

(11) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(12) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether

maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Disclosure to consumer reporting agencies:**

Disclosures pursuant to 5 U.S.C. 552a(b)(12). Disclosures of debt information concerning a claim against an individual may be made from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Paper records and electronic media.

**Retrievability:**

Records are retrievable by the name of the person to whom they apply and/or by case number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of a background investigation, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Paper records are maintained and disposed of in accordance with a record disposition schedule approved by the National Archives and Records Administration. TIGTA is in the process of requesting approval for a record retention schedule for electronic records maintained in this system. These electronic records will not be destroyed until TIGTA receives such approval.

**System manager(s) and address:**

Office of Chief Counsel, TIGTA, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records in this system are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2). Non-exempt record source categories include the following: (1) Department of the Treasury personnel and records, (2) The subject of the record, (3) Witnesses, (4) Parties to disputed matters of fact or law, (5) Congressional inquiries, and, (6) Other Federal agencies including, but not limited to, the Office of Personnel Management, the Merit Systems Protection Board, and the Equal Employment Opportunities Commission.

**Exemptions claimed for the system:**

Some of the records in this system are exempt from 5 U.S.C. 552a(c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (d)(5)(e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C.552a(j)(2) and (k)(2). (See 31 CFR 1.36.)

**TREASURY/DO .310**

**System Name:**

TIGTA Chief Counsel Disclosure Branch Records.

**System location:**

Office of Chief Counsel, Disclosure Branch, TIGTA, 1401 H Street, NW, Washington, DC 20005.

**Categories of individuals covered by the system:**

(1) Requestors for access and amendment pursuant to the Privacy Act of 1974, 5 U.S.C. 552a; (2) Subjects of requests for disclosure of records; (3) Requestors for access to records pursuant to 26 U.S.C. 6103; (4) TIGTA employees who have been subpoenaed or requested to produce TIGTA documents or testimony on behalf of TIGTA in judicial or administrative

proceedings; (5) Subjects of investigations who have been referred to another law enforcement authority; (6) Subjects of investigations who are parties to a judicial or administrative proceeding in which testimony of TIGTA employees or production of TIGTA documents has been sought; and, (7) Individuals initiating correspondence or inquiries processed or controlled by the Disclosure Section.

**Categories of records in the system:**

(1) Requests for access to and/or amendment of records, (2) Responses to such requests, (3) Records processed and released in response to such requests, (4) Processing records, (5) Requests or subpoenas for testimony, (6) Testimony authorizations, (7) Referral letters, (8) Documents referred, (9) Record of disclosure forms, and (10) Other supporting documentation.

**Authority for maintenance of the system:**

5 U.S.C. 301 and 552a, 26 U.S.C 6103, and 31 CFR 1.11.

**Purpose(s):**

The purpose of this system is to enable compliance with applicable Federal disclosure laws and regulations, including statutory record-keeping requirements. In addition, this system will be used to maintain records obtained and/or generated for purposes of responding to requests for access, amendment, and disclosure of TIGTA records.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for

enforcing, or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law, or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when: (a) The agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to an investigation or matter under consideration.

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to Section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3, and

(10) To appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Paper records and/or electronic media.

**Retrievability:**

Name of the requestor, name of the subject of the investigation, and/or name of the employee requested to produce documents or to testify.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

TIGTA is in the process of requesting approval for a record retention schedule for records maintained in this system. These records will not be destroyed until TIGTA receives such approval.

**System manager(s) and address:**

Chief Counsel, TIGTA, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records in this system are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2). Non-exempt record source categories include the following: (1) Department of the Treasury personnel and records, (2) Incoming requests, and (3) Subpoenas and requests for records and/or testimony.

**Exemptions claimed for the system:**

This system may contain records that are exempt from 5 U.S.C. 552a(c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2),(e)(3),(e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). (See 31 CFR 1.36.)

**TREASURY/DO .311**

**System name:**

TIGTA Office of Investigations Files.

**System location:**

National Headquarters, Office of Investigations, 1401 H Street, NW, Washington, DC 20005 and Field Division offices listed in Appendix A.

**Categories of individuals covered by the system:**

(1) The subjects or potential subjects of investigations; (2) The subjects of complaints received by TIGTA; (3) Persons who have filed complaints with TIGTA; (4) Confidential informants; and (5) TIGTA Special Agents.

**Categories of records in the system:**

(1) Reports of investigations, which may include, but are not limited to, witness statements, affidavits, transcripts, police reports, photographs, documentation concerning requests and approval for consensual telephone and consensual non-telephone monitoring, the subject's prior criminal record, vehicle maintenance records, medical records, accident reports, insurance policies, and other exhibits and documents collected during an investigation; (2) Status and disposition information concerning a complaint or investigation including prosecutive action and/or administrative action; (3) Complaints or requests to investigate; (4) General case materials and documentation including, but not limited to, Chronological Case Worksheets (CCW), fact sheets, agent work papers, Record of Disclosure forms, and other case management documentation; (5) Subpoenas and evidence obtained in response to a subpoena; (6) Evidence logs; (7) Pen registers; (8) Correspondence; (9) Records of seized money and/or property; (10) Reports of laboratory examination, photographs, and evidentiary reports; (11) Digital image files of physical evidence; (12) Documents generated for purposes of TIGTA's undercover activities; (13) Documents pertaining to the identity of confidential informants; and (14) Other documents collected and/or generated by the Office of Investigations during the course of official duties.

**Authority for maintenance of the system:**

5 U.S.C. app. 3 and 5 U.S.C. 301.

**Purpose(s):**

The purpose of this system of records is to maintain information relevant to complaints received by TIGTA and collected as part of investigations conducted by TIGTA's Office of Investigations. This system also includes investigative material compiled by the IRS's

Office of the Chief Inspector, which was previously maintained in the following systems of records: Treasury/IRS 60.001-60.007 and 60.009-60.010.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Records other than returns and return information may be used to:

(1) Disclose pertinent information to appropriate federal, state, local, or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law or regulation;

(2) Disclose information to a federal, state, local, or other public authority maintaining civil, criminal, or other relevant enforcement information or other pertinent information that has requested information relevant to or necessary to the requesting agency's, bureau's, or authority's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(3) Disclose information in a proceeding before a court, adjudicative body, or other administrative body before which TIGTA is authorized to appear when (a) the agency, or (b) any employee of the agency in his or her official capacity, or (c) any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee, or (d) the United States, when the agency determines that litigation is likely to affect the agency, is a party to litigation or has an interest in such litigation, and the use of such records by the agency is deemed to be relevant and necessary to the litigation or administrative proceeding and not otherwise privileged;

(4) Disclose information to a court, magistrate or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witness in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a court order where arguably relevant to a proceeding;

(5) Disclose information to the Department of Justice for the purpose of litigating an action or seeking legal advice;

(6) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(7) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(8) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2;

(9) Disclose information to the Equal Employment Opportunity Commission, Merit Systems Protection Board, arbitrators, and other parties responsible for processing personnel actions or conducting administrative hearings or appeals, or if needed in the performance of other authorized duties;

(10) In situations involving an imminent danger of death or physical injury, disclose relevant information to an individual or individuals who are in danger; and

(11) Provide information to other Offices of Inspectors General, the President's Council on Integrity and Efficiency, and the Department of Justice, in connection with their review of TIGTA's exercise of statutory law enforcement authority, pursuant to section 6(e) of the Inspector General Act of 1978, as amended, 5 U.S.C.A. Appendix 3; and,

(12) Disclose information to complainants, victims, or their representatives (defined for purposes here to be a complainant's or victim's legal counsel or a Senator or Representative whose assistance the complainant or victim has solicited) concerning the status and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim, including, once the investigative subject has exhausted all reasonable appeals, any action taken. Information concerning the status of the investigation or case is limited strictly to whether the investigation or case is open or closed. Information concerning the results of the investigation or case is limited strictly to whether the allegations made in the complaint were substantiated or were not substantiated and, if the subject has exhausted all reasonable appeals, any action taken.

(13) Disclose information to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and dispensing of records in the system:**

**Storage:**

Paper records and electronic media.

**Retrievability:**

By name, Social Security Number, and/or case number.

**Safeguards:**

The records are accessible to TIGTA personnel, all of whom have been the subject of background investigations, on a need-to-know basis. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed; these terminals are accessible only to authorized persons. Paper records are maintained in locked facilities and/or cabinets with restricted access.

**Retention and disposal:**

Some of the records in this system are maintained and disposed of in accordance with a record disposition schedule approved by the National Archives and Records Administration. TIGTA is in the process of requesting approval of new records schedules concerning all records in this system of records. Records not currently covered by an approved record retention schedule will not be destroyed until TIGTA receives the National Archives and Records Administration.

**System manager(s) and address:**

Deputy Inspector General for Investigations, Office of Investigations, TIGTA, 1401 H Street, NW, Washington, DC 20005.

**Notification procedure:**

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, subpart C, appendix A. Written inquiries should be addressed to

the Office of Chief Counsel, Disclosure Branch, Treasury Inspector General for Tax Administration, 1401 H Street, NW, Room 469, Washington, DC 20005. This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2).

**Record access procedures:**

See "Notification Procedures" above.

**Contesting record procedures:**

See "Notification Procedures" above.

**Record source categories:**

Some records contained within this system of records are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C. 552a(j)(2) and (k)(2). Non-exempt record source categories include the following: Department of the Treasury personnel and records, complainants, witnesses, governmental agencies, tax returns and related documents, subjects of investigations, persons acquainted with the individual under investigation, third party witnesses, Notices of Federal Tax Liens, court documents, property records, newspapers or periodicals, financial institutions and other business records, medical records, and insurance companies.

**Exemptions claimed for the system:**

Some records contained within this system of records are exempt from 5 U.S.C. 552a(c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). (See 31 CFR 1.36)

**Appendix A--Office of Investigations, TIGTA**

Field Division SAC Offices

Treasury IG for Tax Administration, 401 West Peachtree St., Atlanta, GA 30308.

Treasury IG for Tax Administration, 230 S. Dearborn St., IL 60604.

Treasury IG for Tax Administration, 1919 Smith Street, Houston, TX 77002.

Treasury IG for Tax Administration, 1999 Broadway, Denver, CO 80202.

Treasury IG for Tax Administration, 201 Varick Street, New York, NY 10014.

Treasury IG for Tax Administration, Ronald Dellums Federal Bldg., 1301 Clay Street, Oakland, CA 94612.

Treasury IG for Tax Administration, 2970 Market Street, Philadelphia, PA 19104.

Treasury IG for Tax Administration, 12119 Indian Creek Court, Beltsville, MD 20705.

Appendix B--Audit Field Offices, TIGTA

Treasury IG for Tax Administration, 310 Lowell Street, Andover, MA 01812.

Treasury IG for Tax Administration, 401 W. Peachtree St., Atlanta, GA 30308-3539.

Treasury IG for Tax Administration, Atlanta Service Center, 4800 Buford Highway, Chamblee, GA 30341.

Treasury IG for Tax Administration, 3651 South Interstate 35, Austin, TX 78741.

Treasury IG for Tax Administration, 31 Hopkins Plaza, Fallon Federal Building, Baltimore, MD 21201.

Treasury IG for Tax Administration, 1040 Waverly Ave, Holtsville, NY 11742.

Treasury IG for Tax Administration, 200 W Adams, Chicago, IL 60606.

Treasury IG for Tax Administration, Peck Federal Office Bldg., 550 Main Street, Room 5028, Cincinnati, OH 45201.

Treasury IG for Tax Administration, 4050 Alpha Road, Dallas, TX 75244.

Treasury IG for Tax Administration, 600 17th Street, Denver, CO 80202.

Treasury IG for Tax Administration, Fresno Service Center, 5045 E. Butler Stop 11, Fresno, CA 93727.

Treasury IG for Tax Administration, 7850 SW 6th Court, Plantation, FL 33324.

Treasury IG for Tax Administration, 333 West Pershing Road, Kansas City, MO 64108.

Treasury Inspector General for Tax Administration--Audit, 24000 Avila Road, Laguna Niguel, CA 92677.

Treasury IG for Tax Administration, 300 N. Los Angeles Street, Los Angeles, CA 90012.

Treasury IG for Tax Administration, 5333 Getwell Rd, Memphis, TN 38118.

Treasury IG for Tax Administration, 1160 West 1200 South, Ogden, Utah 84201.

Treasury IG for Tax Administration, Federal Office Building, 600 Arch Street, Philadelphia, PA 19106.

Treasury IG for Tax Administration, 915 2nd Avenue, Seattle, WA 98174.

Treasury IG for Tax Administration, 1222 Spruce, St. Louis, MO 63103.

Treasury IG for Tax Administration, 92 Montvale Avenue, Stoneham, MA 02180.

Treasury IG for Tax Administration, Ronald Dellums Federal Bldg., 1301 Clay Street, Oakland, CA 94612.

**TREASURY/DO .411**

**System name:** Intelligence Enterprise Files

**System location:** The Office of Intelligence and Analysis (OIA), Department of the Treasury, Washington, DC. The system may be accessed by Departmental personnel in other components of the Treasury Department with the permission of OIA, provided that such personnel are

determined by OIA to have the requisite security clearance and the need to know information maintained in the system.

**Categories of individuals covered by the system:**

(1) Individuals related to:

A. The capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, international terrorists, international narcotics traffickers, members of transnational criminal organizations, proliferators of weapons of mass destruction, and their associates, supporters, and facilitators;

B. Foreign financial and economic activities pertaining to national security;

C. Activities constituting a threat to the national security, foreign policy, or the economy of the United States, or that are preparatory to, facilitate, or support such activities, including:

i. Financial crimes, including money laundering, unlicensed money transmission, evading reporting requirements, access device fraud, financial institution fraud, and activities affecting the safety or soundness of financial institutions, in accordance with Title 18 and Title 31 of the United States Code;

ii. Suspicious financial transactions and other data required to be reported by the Bank Secrecy Act, 31 U.S.C. 5311 *et seq.*, because they have a high degree of usefulness in the conduct of intelligence or counterintelligence activities or for other national security purposes;

iii. Transactions related to individuals subject to or under consideration for the imposition of economic sanctions;

iv. Activities that could reasonably be expected to assist in the development of a weapon of mass destruction, including attempts to import, procure, possess, store, develop, or transport nuclear or radiological material;

v. Activities against or threats to the United States or U.S. persons and interests by foreign or international terrorist groups or individuals involved in terrorism;

vi. Activities to identify, create, exploit, or undermine vulnerabilities of the Treasury Department's information systems and national security systems infrastructure;

vii. Activities, not wholly conducted within the United States, which violate or may violate the laws that prohibit the production, transfer, or sale of narcotics or substances controlled in accordance with Title 21 of the United States Code, or those associated activities otherwise prohibited by Titles 21 and 46 of the United States Code;

viii. Activities, not wholly conducted within the United States, which otherwise violate or may violate United States or foreign criminal laws;

ix. Activities, not wholly conducted within the United States, that constitute genocide, mass atrocities, or other grave breaches of human rights;

x. Activities that impact or concern the security, safety, and integrity of our

international borders, such as those that may constitute violations of the immigration or customs laws of the United States;

D. Espionage, the improper release of sensitive or classified information, sabotage, assassination, or other intelligence activities conducted by or on behalf of foreign powers, organizations, persons, or their agents, or international terrorist organizations, international narcotics traffickers, members of transnational criminal organizations, proliferators of weapons of mass destruction, and their associates, supporters, and facilitators;

E. Activities where the health or safety of an individual may be threatened;

F. Information necessary for the provision of intelligence support to the Treasury Department.

(2) Individuals who voluntarily request assistance or information, through any means, from OIA, and individuals who consent to providing information, which may relate to a threat or otherwise affect the national security of the United States.

(3) Individuals who are or have been associated with Treasury Department or OIA activities or with the administration of the Department of the Treasury, including information about individuals that is otherwise required to be maintained by law.

**Categories of records in the system:**

(1) Records containing classified and unclassified intelligence information, counterintelligence information, counterterrorism information, and information, including records pertaining to law enforcement that are related to national security. This includes source records and other

forms of "raw" intelligence as well as the analysis of this information, obtained from all entities of the Federal government, including the Intelligence Community; foreign governments, persons, or other entities including international organizations; and state, local, tribal, and territorial government agencies.

(2) Records containing information pertaining to OIA's responsibilities overtly collected from record subjects, individual members of the public, and private sector entities.

(3) Records containing information reported pursuant to and maintained consistent with the Bank Secrecy Act.

(4) Records containing information pertaining to the imposition and enforcement of economic sanctions, including reports pursuant to chapter V of Title 31, Code of Federal Regulations, and information provided through license applications, requests to have funds unblocked, and requests for reconsideration of a designation.

(5) Records containing information obtained from Intelligence Community elements or other entities about individuals who are or may be engaged in activities related to terrorism, transnational narcotics trafficking, transnational criminal organizations, the proliferation of weapons of mass destruction, or other threats to the national security, economy, or foreign policy of the United States.

(6) Records containing law enforcement or other information received from other government agencies pertaining to potential threats to the national security, the economy, or foreign policy of the United States.

(7) Records containing operational and administrative records, including correspondence

records.

(8) Records containing information related to or obtained to ensure the security of the Treasury Department, including through authorized physical, personnel, information systems security, and insider threat investigations, inquiries, analysis, and reporting.

(9) Records contain publicly available information, related to lawful OIA activities, about individuals as derived from media, including periodicals, newspapers, broadcast transcripts, and other public reports and computer databases, including those available by subscription to the public.

(10) Records about individuals who voluntarily provide any information contained within the system.

**Authority for maintenance of the system:** 5 U.S.C. 301; 31 U.S.C. 311-312; Executive Orders 12333, 12968, 13388, and 13526, as amended.

**Purpose(s):** The records in this system will be used to fulfill OIA's statutory and Executive Order mandates to collect (overtly or through publicly-available sources), receive, analyze, collate, produce, and disseminate information, intelligence, and counterintelligence related to the operations and responsibilities of the entire Department, including all components and bureaus. The system will allow OIA to carry out its functions of discharging its responsibilities while building a robust analytical capability on terrorist financing; coordinating and overseeing the work of intelligence analysts in Treasury Department components; focusing intelligence efforts on the highest priorities of the Department; ensuring that the intelligence needs of OFAC and FinCEN are met; and providing intelligence support to senior Department officials on a wide range of international economic and other relevant issues.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

These records may be used to disclose pertinent information to:

(1) Any United States, foreign, or multinational government or agency, or private sector individual or organization, with responsibilities relating to the national security, economy, or foreign policy of the United States, including responsibilities related to the implementation of or compliance with applicable authorities, to analyze, counter, deter, or prevent threats related to foreign intelligence or counterintelligence activities, terrorism, international narcotics traffickers, transnational criminal organizations, or proliferators of weapons of mass destruction;

(2) Any United States, foreign, or multinational government or agency with the responsibility and authority for investigating, prosecuting, or otherwise enforcing a civil or criminal law, regulation, rule, order, or contract, where the information on its face or when combined with other information indicates a potential violation of any such law, regulation, rule, order, or contract enforced by that government or agency;

(3) Any Federal banking agency when OIA believes that the information raises significant concerns regarding the safety or soundness of any depository institution doing business in the United States;

(4) Any United States agency, including Federal banking agencies, where the information is relevant to such agency's supervisory responsibilities;

(5) Any United States, foreign, or multinational government or agency, or other entity, including private sector individuals and organizations, where disclosure is in furtherance of the Treasury Department's or OIA's information-sharing responsibilities under the

National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, Executive Order 12333, as amended, or any successor order, statute, national security directive, intelligence community directive, or other directive, or any classified or unclassified implementing procedures promulgated pursuant to such orders and directives;

(6) Any U.S. agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, national security, law enforcement or law enforcement intelligence, or other information, where disclosure is undertaken for intelligence, counterterrorism, national security, insider threat, or related law enforcement purposes, as authorized by United States law or Executive orders;

(7) Any other element of the Intelligence Community, as defined by Executive Order 12333, as amended, or any successor order, for the purpose of allowing that agency to determine whether the information is relevant to its responsibilities and can be retained by it;

(8) Any United States, foreign, or multinational government or agency, or private sector individual or organization, with responsibility for imposing and enforcing economic sanctions or for complying with or implementing economic sanctions, for the purpose of carrying out such responsibility;

(9) Any United States agency with responsibility for activities related to counterintelligence or the detection of insider threats, for the purpose of conducting such activities;

(10) Any United States, foreign, or multinational government or agency, if the information is relevant to the requesting entity's decision or to a Treasury Department decision

concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit;

(11) Any foreign persons or foreign government agencies, international organizations, and multinational agencies or entities, including private entities, under circumstances or for purposes mandated by, imposed by, or conferred in, Federal statute, treaty, or other international agreement or arrangement in accordance with OIA's authorities;

(12) Any individual, organization, or entity, as appropriate, for the purpose of guarding it against or responding to an actual or potential serious threat, to the extent the information is relevant to the protection of life, health, or property;

(13) Representatives of the Department of Justice or other United States entities, to the extent necessary to obtain their advice on any matter that is within their official responsibilities to provide;

(14) Any federal agency, a court, or a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the Federal Government is a party to the judicial or administrative proceeding. In those cases where the Federal Government is not a party to the proceeding, records may be disclosed pursuant to a subpoena by a court, agency, or other entity of competent jurisdiction where arguably relevant to a proceeding or in connection with a criminal proceeding;

(15) The Department of Justice (DOJ) for the purpose of receiving legal advice and representation;

(16) Contractors, grantees, experts, consultants, interns, volunteers and others (including agents of the foregoing) performing or working on a contract, service, grant, cooperative

agreement, or other assignment for the Treasury Department, when necessary to accomplish such function;

(17) Individual members or staff of the United States Senate Select Committee on Intelligence, the United States Senate Committee on Banking, Housing, and Urban Affairs, the United States House Permanent Select Committee on Intelligence, and the United States House Committee on Financial Services in connection with the exercise of their oversight and legislative functions;

(18) The National Archives and Records Administration (NARA), for the purpose of records management;

(19) Any agency, organization, or individual for the purposes of performing audit or oversight of the Treasury Department or OIA, as authorized by law and as necessary and relevant to such audit or oversight function;

(20) The President's Foreign Intelligence Advisory Board, the Intelligence Oversight Board, any successor organizations, and any intelligence or national security oversight entities established by the President, when the Assistant Secretary for Intelligence and Analysis determines that disclosure will assist these entities in the performance of their oversight functions;

(21) Agencies, entities, and persons when: (1) the Treasury Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that

rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are stored electronically or on paper in secure facilities. The records are stored in file folders or on magnetic discs, tapes, or electronic media.

**Retrievability:**

Data may be retrieved by an individual's name or other identifier, such as Social Security number, phone number, or case number.

**Safeguards:**

Records in electronic and physical form in this system are maintained in secure facilities protected by appropriate physical and technological safeguards with access limited by password or access code only to authorized personnel. Records in this system are safeguarded in accordance with applicable laws, rules, and policies, including Intelligence Community standards, Treasury Department information technology security policies, and the Federal Information Security Management Act. Classified information is stored appropriately in a secured, certified, and accredited facility, in secured databases and containers, and in accordance with other applicable requirements, including those pertaining to classified information. The system incorporates logging functions that facilitate the auditing of individual use and access.

**Retention and disposal:**

Records will be retained and disposed of in accordance with a records retention and disposal schedule to be submitted to and approved by NARA.

**System manager(s) and address:**

Director of Intelligence Information Systems, Office of Intelligence and Analysis, Department of the Treasury, 1500 Pennsylvania Ave. NW, Washington, DC 20220.

**Notification procedure:**

This system of records contains classified and controlled unclassified information related to intelligence, counterintelligence, national security, and law enforcement programs. As a result, records in this system have been exempted from notification, access, and amendment to the extent permitted by the Privacy Act, 5 U.S.C. 552a(k).

In accordance with 31 CFR Part 1, subpart C, Appendix A, individuals wishing to be notified if they are named in non-exempt records in this system of records, to gain access to such records maintained in this system, or seek to contest the content of such records, must submit a written request containing the following elements: (1) identify the record system; (2) identify the category and type of records sought; and (3) provide at least two items of secondary identification. Address inquiries to: Privacy Act Request, DO, Director, Disclosure Services, Department of the Treasury, 1500 Pennsylvania Ave. NW, Washington, DC 20220.

**Record access procedures:**

See "NOTIFICATION PROCEDURES" above.

**Contesting record procedures:**

See "NOTIFICATION PROCEDURES" above.

**Record source categories:**

Information contained in this system is obtained from individuals; other government, non-government, commercial, public, and private agencies and organizations, both domestic and foreign; media, including periodicals, newspapers, broadcast transcripts, and publicly-available databases; intelligence source documents; investigative reports; and correspondence.

**Exemptions claimed for the system:**

Records in this system related to classified and controlled unclassified information related to intelligence, counterintelligence, national security, and law enforcement programs are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1). See 31 CFR 1.36.

[FR Doc. 2016-26663 Filed: 11/4/2016 8:45 am; Publication Date: 11/7/2016]