Privacy and Civil Liberties Impact Assessment for the

Treasury eComplaints

July 15, 2016

Reviewing Official
Timothy H. Skinner
Director, Privacy and Civil Liberties
Department of the Treasury
Washington DC 20220

Bureau Certifying Official
Timothy H. Skinner
Director, Privacy and Civil Liberties
Department of the Treasury
Washington DC 20220

Section 1: Introduction

It is the policy of the Department of the Treasury ("Treasury" or "Department") and its Bureaus to conduct a Privacy and Civil Liberties Impact Assessment ("PCLIA") when personally identifiable information ("PII") is maintained in a system or by a project. PCLIAs are required for all systems and projects that collect, maintain, or disseminate PII, regardless of the manner in which the information is retrieved.

This assessment is being completed pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget ("OMB") Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before:

1. developing or procuring information technology ("IT") systems or projects that collect, maintain or disseminate PII from or about members of the public, or

2. initiating a new collection of information that: a) will be collected, maintained, or disseminated using IT; and b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons. Agencies, instrumentalities, or employees of the federal government are not included.

This PCLIA provides the following information regarding the system or project:

(1) an overview of its purpose and functions;
(2) a description of the information collected;
(3) a description of the how information is maintained, used, and shared;
(4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and
(5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

A PCLIA is being done for the first time on this system since system ownership was transferred from the Internal Revenue Service (IRS) to Treasury's Departmental Offices (DO). The eComplaints system was previously housed at the IRS which did a Privacy Impact Assessment on the system at that time (under the system name I-Trak). This is the first time Treasury DO has completed a PCLIA for the system under its new name, eComplaints.

Section 2: Definitions

Agency – means any entity that falls within the definition of the term "executive agency" as defined in 31 U.S.C. § 102.

Certifying Official – The Bureau Privacy and Civil Liberties Officer(s) who certify that all requirements in TD and TD P 25-07 have been completed so a PCLIA can be reviewed and approved by the Treasury Deputy Assistant Secretary for Privacy, Transparency, and Records.

Collect (including "collection") – means the retrieval, receipt, gathering, or acquisition of any PII and its storage or presence in a Treasury system. This term should be given its broadest possible meaning.

Contractors and service providers – are private companies that provide goods or services under a contract with the Department of the Treasury or one of its bureaus. This includes, but is not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

Data mining – means a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where **–** (a) a department or agency of the federal government, or a non-federal entity acting on behalf of the federal government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely **–** (i) the detection of fraud, waste, or abuse in a government agency or program; or (ii) the security of a government computer system.

Disclosure – When it is clear from its usage that the term "disclosure" refers to records provided to the public in response to a request under the Freedom of Information Act (5 U.S.C. § 552, "FOIA") or the Privacy Act (5 U.S.C. § 552a), its application should be limited in that manner. Otherwise, the term should be interpreted as synonymous with the terms "sharing" and "dissemination" as defined in this manual.

Dissemination – as used in this manual, is synonymous with the terms "sharing" and "disclosure" (unless it is clear from the context that the use of the term "disclosure" refers to a FOIA/Privacy Act disclosure).

E-Government – means the use of digital technologies to transform government operations to improve effectiveness, efficiency, and service delivery.

Federal information system – means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information owned or under the control of a federal agency, whether automated or manual.

Final Rule – After the NPRM comment period closes, the agency reviews and analyzes the comments received (if any). The agency has the option to proceed with the rulemaking as proposed, issue a new or modified proposal, or withdraw the proposal before reaching its final decision. The agency can also revise the supporting analyses contained in the NPRM (e.g., to address a concern raised by a member of the public in response to the NPRM).

Government information – means information created, collected, used, maintained, processed, disseminated, or disposed of by or for the federal government.

Individual – means a citizen of the United States or an alien lawfully admitted for permanent residence. If a question does not specifically inquire about or an issue does not clearly involve a Privacy Act system of records, the term should be given its common, everyday meaning. In certain contexts, the term individual may also include citizens of other countries who are covered by the terms of an international or other agreement that involves information stored in the system or used by the project.

Information – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. This term includes, but is not limit to, information contained in a Privacy Act system of records.

Information technology (IT) – means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).

Major Information system – embraces "large" and "sensitive" information systems and means "a system or project that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources." OMB Circular A-130, § 6.u. This definition includes all systems that contain PII and are rated as "MODERATE or HIGH impact" under Federal Information Processing Standard 199.

National Security systems – a telecommunications or information system operated by the federal government, the function, operation or use of which involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management. Clinger-Cohen Act of 1996, 40 U.S.C. § 11103.

Notice of Proposed Rule Making (NPRM) – the Privacy Act (Section (J) and (k)) allow agencies to use the rulemaking process to exempt particular systems of records from some of the requirements in the Act. This process is often referred to as "notice-and-comment rulemaking." The agency publishes an NPRM to notify the public that the agency is proposing a rule and provides an opportunity for the public to comment on the proposal before the agency can issue a final rule.

Personally Identifiable Information (PII) –any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Privacy and Civil Liberties Impact Assessment (PCLIA) – a PCLIA is:

(1) a *process* conducted to: (a) identify privacy and civil liberties risks in systems, programs, and other activities that maintain PII; (b) ensure that information systems**,** programs, and other activities comply with legal, regulatory, and policy requirements; (c) analyze the privacy and civil liberties risks identified; (d) identify remedies, protections, and alternative or additional privacy controls necessary to mitigate those risks; and (e) provide notice to the public of privacy and civil liberties protection practices.
(2) a *document* that catalogues the outcome of that privacy and civil liberties risk assessment process.

Protected Information – as the term is used in this PCLIA, has the same definition given to that term in TD 25-10, Section 4.

Privacy Act Record – any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. 5 U.S.C. § 552a (a)(4).

Reviewing Official – The Deputy Assistant Secretary for Privacy, Transparency, and Records who reviews and approves all PCLIAs as part of her/his duties as a direct report to the Treasury Senior Agency Official for Privacy.

Routine Use – with respect to the disclosure of a record outside of Treasury (i.e., external sharing), the sharing of such record for a purpose which is compatible with the purpose for which it was collected 5 U.S.C. § 552a(a)(7).

Sharing – any Treasury initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of Treasury information, regardless of whether it is covered by the Privacy Act. It does not include responses to requests for agency records under FOIA or the Privacy Act. It is synonymous with the term "dissemination" as used in this assessment. It is also synonymous with the term "disclosure" as used in this assessment unless it is clear from the context in which the term is used that it refers to disclosure to the public in response to a request for agency records under FOIA or the Privacy Act.

System – as the term used in this manual, includes both federal information systems and information technology.

System of Records – a group of any records under the control of Treasury from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. 5 U.S.C. § 552a (a)(5).

System of Records Notice – Each agency that maintains a system of records shall publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records, which notice shall include: (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at her/his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at her/his request how she/he can gain access to any record pertaining to him contained in the system of records, and how she/he can contest its content; and (I) the categories of sources of records in the system. 5 U.S.C. § 552a (e)(4).

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

Section 3: System Overview

Section 3.1: System/Project Description and Purpose

eComplaints is one of two systems used to process Equal Employment Opportunity (EEO) counseling consultations and case management information: (1) iComplaints; and (2) eComplaints. The iComplaints system is discussed here for purposes of background only because it is covered by a separate PCLIA.

(1) ***iComplaints*** *(the subject of a separate PCLIA): The purpose of the Treasury iComplaints system is to process, manage, and report information related to, departmentwide administrative EEO cases as well as to provide aggregate EEO data for internal reports (including form 462 "Report to the Equal Employment Opportunity Commission (EEOC)"). iComplaints also maintains reports from EEO counseling sessions, acceptance/acknowledgement letters (wherein the agency acknowledges receipt of a formal EEO complaint) and final agency decisions (FAD) (if one is issued). Participation in an informal/counseling stage is a prerequisite before filing a formal EEO complaint. EEO counseling sessions consist of meetings between an EEO counselor and the individual who wishes to obtain information regarding possible EEO violations, obtaining facts relevant to a possible claim, obtaining management's version of the facts, and advising the individual on whether his or her allegations could be enough to state a claim. During this stage, OCRD provides individuals with information about their EEO rights and responsibilities and, when possible, strives to achieve informal resolution of the individual's concerns or issues. This counseling session results in the completion of a "Report of Counseling" form which is used to capture the employee's allegations and management's response. This document is then uploaded into iComplaints. If a resolution cannot be achieved in the informal stage, the individual may file a formal EEO complaint. Formal EEO complaints are not, however, maintained in iComplaints. Formal complaints and documentation related to the resolution of those complaints are maintained in "eComplaints," a separate OCRD system that is the subject of this PCLIA.*

(2) ***eComplaints*** *(the subject of this PCLIA): is the system used to produce and store EEO administrative complaint files and documents used in adjudicating formal EEO complaints. Individual Complaints of Employment Discrimination With the Department of the Treasury, the EEO Report of Counseling, At the initial stage of OCRD's involvement, a Report of Counseling and an employee's formal complaint are uploaded to eComplaints. At this stage, OCRD will determine if the case should be dismissed for procedural reasons (e.g., missing the filing deadline), or accepted for investigation. If dismissed, OCRD writes a procedural dismissal that is uploaded and sent to the complainant along with appeal rights (described below). If the complaint is accepted, complaint documentation is mailed to the United States Postal Service's (USPS) contract investigations service (pursuant to a multi-agency investigative services contract) which then forwards the file to a USPS contract investigator. After completion of the*

investigation, USPS returns the results to OCRD by postal mail (containing a hard copy and CD) within approximately 180 days. The investigative file is then uploaded into eComplaints.

After the investigation is completed, the complainant is given the option of either having the matter adjudicated by OCRD or the EEOC. If the complainant chooses to have his or her complaint adjudicated by OCRD, the agency issues a final agency decision (FAD) based on the investigative record with a determination as to whether discrimination occurred. If the agency determines discrimination occurred, it will order relief for the complainant. The FAD is then uploaded to both the iComplaints and eComplaints systems.

If the complainant elects to pursue a hearing before the EEOC, the case is heard by an Administrative Judge who will make a decision and order relief if the judge determines discrimination occurred. This decision is then sent back to the agency which has 40 days to issue a final order stating whether the agency agrees with the Administrative Judge and whether it will grant the relief ordered. This final order, and the FAD, provide information about the complainant's right to appeal the final decision to EEOC, the right to file a civil action in federal district court, and the deadline for filing both an appeal and a civil action.

The complainant (or the agency) then has 30 days after receipt of the FAD or the final order to file an appeal to the EEOC Office of Federal Operations. EEOC appellate attorneys then review the entire file, including the agency's investigation, the FAD or decision of the Administrative Judge, the transcript of what was said at the hearing (if there was a hearing) and any statements made on appeal.

When the agency takes an adverse action against an employee, the employee also has the option of appealing the action to the Merit Systems Protection Board (MSPB). MSPB is an independent, quasi-judicial agency in the Executive branch of the Federal Government that serves as the guardian of Federal merit systems. The Board is composed of three members who are appointed by the President and confirmed by the Senate. In addition to other cases, the MSPB hears cases where an employee alleges discrimination in connection with the adverse personnel action. MSPB only hears cases listed at 5 CFR 1201.3(a). If the employee alleges issues both within and outside MSPB's jurisdiction, the employee may split his or her claims between the EEOC and MSPB processes. See the EEOC regulations found at 29 CFR Part 1614 and the EEOC guidance at Management Directive 110 for a further explanation of the Federal EEO complaints process.

Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project		
☐ **0 – 999**	☒ **1000 – 9,999**	☐ **10,000 – 99,999**
☐ **100,000 – 499,999**	☐ **500,000 – 999,999**	☐ **1,000,000+**

Section 3.2: Authority to Collect

The authority for operating this system or performing this project is found in:

- 29 CFR Part 1614, which directs and authorizes the Department to maintain a continuing program to promote equal opportunity and to identify and eliminate discriminatory practices and policies. Part of this mandate requires providing sufficient resources to ensure efficient and successful operation of the program and to provide for the prompt, fair and impartial processing of complaints. 29 CFR § 1614.102(a)(1)-(2).
- Title VII of the Civil Rights Act of 1964 (Title VII), as amended, 42 U.S.C. 2000e-16
- The Equal Pay Act, 29 U.S.C. 206(d)
- The Rehabilitation Act of 1973, 29 U.S.C. 791
- The Americans with Disabilities Act, as amended
- The Age Discrimination in Employment Act of 1967 (ADEA), as amended, 29 U.S.C. § 633a
- Title II of the Genetic Information Nondiscrimination Act (GINA), 42 U.S.C. 2000ff
- Reorg. Plan No. 1 of 1978, 43 FR 19607 (May 9, 1978) and Exec. Order No. 12106, 44 FR 1053 (Jan. 3, 1979)
- The Federal Sector Equal Employment Opportunity (EEO) Regulations, 29 C.F.R. Part 1614
- Treasury Order 102-02
- Treasury Directive 12-41
- Executive Order 11478

Authority	Description

Section 4: Information Collection

Section 4.1: Relevant and Necessary

The Privacy Act requires "each agency that maintains a system of records [to] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be fulfilled by statute or by executive order of the President." 5 U.S.C. § 552a (e)(1). It allows federal agencies to exempt records from certain requirements (including the relevant and necessary requirement) under certain conditions5 U.S.C. §552a (k). The proposed exemption must be described in a Notice of Proposed Rulemaking ("NPRM"). In the context of the Privacy Act, the purpose of the NPRM is to give the public notice of a Privacy Act exemption claimed for a system of records and solicit public opinion on the proposed exemption. After addressing any public concerns raised in response to the NPRM, the agency must issue a Final Rule. It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final Rule process.

Section 4.1(a) Please check all of the following that are true:

1. ☐ None of the PII maintained in the system or by the project is part of a Privacy Act system of records;
2. ☐ All of the PII maintained in the system or by the project is part of a system of records and none of it is

exempt from the Privacy Act relevant and necessary requirement;

3. ☐ All of the PII maintained in the system or by the project is part of a system of records and all of it is exempt from the Privacy Act relevant and necessary requirement;
4. ☒ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and the records to which the Privacy Act applies are exempt from the relevant and necessary requirement; and
5. ☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and none of the records to which the Privacy Act applies are exempt from the relevant and necessary requirement.

Section 4.1(b) ☒ Yes ☐ No ☐ N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, was an assessment conducted prior to collection (e.g., during Paperwork Reduction Act analysis) to determine which PII types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements?

Section 4.1(c) ☒ Yes ☐ No ☐ N/A With respect to PII currently maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is the PII limited to only that which is relevant and necessary to meet the system's or project's mission requirements?

Section 4.1(d) ☒ Yes ☐ No With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement is there a process to continuously reevaluate and ensure that the PII remains relevant and necessary?

Certain records in this system are exempt from Section (e)(1) (requiring that agencies maintain only relevant and necessary information) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). See 31 CFR 1.36.

Certain (not all) files within this system of records contain information obtained by OCRD in the course of investigations of complaints alleging violations of Title VII of the Civil Rights Act, the Age Discrimination in Employment Act, the Equal Pay Act, the Americans With Disabilities Act and the Rehabilitation Act. In the course of some investigations, OCRD may obtain information regarding unlawful employment practices other than those complained of by the individual who is the subject of the file. It would impede OCRD in performing its mission if the relevant and necessary provision applied to these types of records.

In collecting information during an EEO investigation, it is often impossible or unfeasible to determine relevance and necessity prior to collection of the information. Information that may initially appear irrelevant or unnecessary may, when collated and analyzed with other available information, become more pertinent as an investigation progresses. Similarly, information that appears to be relevant and necessary when collected may reveal itself to be unnecessary as the complaint process progresses and information is obtained from other sources, including the individual about whom the complaint was filed.

Nevertheless, OCRD seeks to collect only information that is relevant and necessary by narrowly tailoring forms in which information is collected and having investigations conducted by individuals who are knowledgeable of EEO matters and can, therefore, generally narrow the collection of information to that which is relevant and necessary to the EEO mission. This is achieved by using forms(Report of Counseling and Individual Complaint of Discrimination with the Department of the Treasury forms) that contain questions that are narrowly tailored to obtain only information necessary for the adjudication of the relevant issues. The investigatory files are assembled by EEO investigators (through the United States Postal Service contract for these services) who are trained to focus soley on information necessary to resolve the relevant issues in a particular discrimination complaint. Final agency decisions (FADs) issued by the agency are also narrowly tailored to contain only information relevant and necessary to resolving the factual and legal issues presented in the case.

eComplaints also contains evidentiary files for the resolution of complaints of violations of the terms of EEO Settlement Agreements and compliance orders, both of which are narrowly tailored to only include information that is necessary and relevant for the adjudication of the Settlement Agreement provision or compliance matter(s) at issue. Occasionally, OCRD will receive a hearing record from the EEOC that will need to be uploaded into eComplaints. This information is narrowly tailored to resolving the complaint.

Section 4.2: PII and/or information types or groupings

To perform their various missions, federal agencies must necessarily collect various types of information. The checked boxes below represent the types of information maintained in the system or by the project. Information identified below is used by the system or project to fulfill the purpose stated in Section 3.3 – Authority to Collect.

Biographical/General Information		
☒ Name (first, last, middle initial)	☒ Gender	☐ Group/Organization Membership
☒ Date of Birth (age)	☒ Race	☐ Military Service Information
☒ Home Physical/Postal Mailing Address	☒ Ethnicity	☒ Personal Home Phone or Fax Number
☒ Zip Code	☒ Personal Cell Number	☐ Alias (including nickname)
☒ Business Physical/Postal Mailing Address	☒ Business Cell Number	☒ Business Phone or Fax Number
☒ Personal e-mail address	☒ Nationality	☐ Mother's Maiden Name
☒ Business e-mail address	☒ Country of Birth	☒ Spouse Information
☐ Personal Financial Information (including loan information)	☒ City or County of Birth	☒ Children Information
☐ Business Financial Information (including loan information)	☒ Immigration Status	☐ Information about other relatives.
☒ Marital Status	☒ Citizenship	☒ Professional/personal references or other information about an individual's friends, associates or acquaintances.
☒ Religion/Religious Preference	☐ Device settings or preferences (e.g., security level, sharing options, ringtones).	☐ Global Positioning System (GPS)/Location Data
☒ Sexual Orientation	☐ User names, avatars etc.	☐ Secure Digital (SD) Card or Other Data stored on a card or other technology
☐ Cell tower records (e.g., logs. user location, time etc.)	☐ Network communications data	☒ Cubical or office number
☐ Contact lists and directories (known to contain personal information)	☐ Contact lists and directories (not known to contain personal information, but uncertain)	☐ Contact lists and directories (known to contain only business information)
☐ Education Information	☒ Resume or curriculum vitae	☒ EEO Counselor Name
☒ Complainant's signature.	☒ Complainant's national origin.	☒ Name of applicant for a Treasury position:
☒ Name, address and the name of the business of Complainant's Representative.	☒ Counselor's signature	☒ Employment status.
☒ Employer alleged to have engaged in discrimination.	☒ Factual background supporting discrimination allegations (can include PII).	☒ Color
☒ Pregnancy (as basis for claim)	☒ LGBT (as basis for claim)	☒ Protected Genetic Information
☒ Parental status (as basis for a claim)	☒ Type of prior EEO complaint activity (as the basis for a claim)	☒

Identifying Numbers	
☐ Full Social Security number	☐ Health Plan Beneficiary Number
☐ Truncated/Partial Social Security number (e.g., last 4 digits)	☐ Alien Registration Number
☐ Personal Taxpayer Identification Number	☐ Business Taxpayer Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Credit Card Number	☐ Business Credit Card Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Vehicle Identification Number	☐ Business Vehicle Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal License Plate Number	☐ Business License Plate Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☒ File/Case ID Number (individual)	☐ File/Case ID Number (business) (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Professional License Number	☐ Business Professional License Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☒ Employee Identification Number	☐ Patient ID Number
☐ Business Bank Account Number	☐ Personal Bank Account Number
☐ Commercially obtained internet navigation/purchasing habits of individuals	☐ Government obtained internet navigation/purchasing habits of individuals
☐ Business License Plate Number (non-sole-proprietor)	☐ Driver's License Number
☐ Personal device identifiers or serial numbers	☐ Other Identifying Numbers (please describe):_____
☐ Passport Number and Passport information (including full name, passport number, DOB, POB, sex, nationality, issuing country photograph and signature) (use "Other" if some but not all elements are collected)	☐ Other Identifying Numbers (please describe):_____

Medical/Emergency Information Regarding Individuals		
☒ Medical/Health Information	☒ Worker's Compensation Act Information	☒ Patient ID Number
☒ Mental Health Information	☒ Disability Information (complainant's – as basis for claim)	☒ Emergency Contact Information (e.g., a third party to contact in case of emergency)
☐ Other (please describe): ___Information regarding medical documentation may be provided by employee if they are seeking a reasonable accommodation through the EEO process. _____		

Biometrics/Distinguishing Features/Characteristics of Individuals		
☒ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) (only gender is collected in eComplaints where applicable)	☒ Signatures (complainant, complainant's representative and counselor)	☐ Vascular scans
☐ Fingerprints	☐ Photos	☐ Retina/Iris Scans
☐ Palm prints	☐ Video	☐ Dental Profile
☐ Voice audio recording	☐ Scars, marks, tattoos	☐ DNA Sample or Profile

☐ Other (please describe): _____	☐ Other (please describe): _____	☐ Other (please describe): _____

Specific Information/File Types		
☐ Taxpayer Information/Tax Return Information	☒ Law Enforcement Information	☒ Security Clearance/Background Check Information
☒ Civil/Criminal History Information/Police Records (government source)	☐ Credit History Information (government source)	☐ Bank Secrecy Act Information
☒ Civil/Criminal History Information/Police Records (commercial source)	☐ Credit History Information (commercial source)	☐ National Security/Classified Information
☐ Protected Information (as defined in Treasury Directive 25-10)	☒ Case files	☒ Personnel Files
☒ Information provided under a confidentiality agreement	☐ Information subject to the terms of an international or other agreement	☒ Other (please describe): The report of EEO counseling, the acknowledgement letter (wherein the agency acknowledges receipt of a formal EEO complaint), the acceptance letter (wherein the agency states the claims asserted that must be investigated), investigatory files, Settlement Agreements, Orders of Relief, and final agency decisions (FADs).

Audit Log and Security Monitoring Information		
☒ User ID assigned to or generated by a user of Treasury IT	☐ Date and time an individual accesses a facility, system, or other IT	☐ Files accessed by a user of Treasury IT (e.g., web navigation habits)
☐ Passwords generated by or assigned to a user of Treasury IT	☐ Internet or other queries run by a user of Treasury IT	☒ Contents of files accessed by a user of Treasury IT
☐ Biometric information used to access Treasury facilities or IT	☐ Video of individuals derived from security cameras	☐ Public Key Information (PKI).
☐ Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT or devices	☐ Still photos of individuals derived from security cameras.	☐ Internet Protocol (IP) Address
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe):

Other	
☐ Other (please describe: _____	☐ Other (please describe: _____
☐ Other (please describe: _____	☐ Other (please describe: _____

Section 4.3: Sources of information and the method and manner of collection

The Individual Who Files an EEO Complaint or Seeks Counseling (Complainant)	The Managers and Witnesses Named in the Complaint and Agency Employment

	Information
Specific PII identified in Section 4.2 that was acquired from this source (where relevant and necessary to investigating a claim): • Name (First, MI, Last) • Employee ID from HRConnect • Date of Birth (age) • Pay Plan • Grade • Job Series • Race • Color • Ethnicity • Gender • Marital status • Employee Type • Occupation • Work email • Personal email • Country • Complainant's National Origin • Bargaining Unit • Union Code • Union Code Translation • Disability Description • Org. Code • Home Address (full) • Home Telephone • Home Fax • Personal Cell Phone • Business Cell Phone • Work Address (full) • Work Telephone • Work Fax • Work Cell • Complainant's signature • Counselor's signature • Complainant's current employment status • Factual background re: claim (including PII) • Protected genetic information • LGBT status • Pregnancy • Parental status • Prior EEO activity (including description) • Name of applicant for Treasury position (non-employee) • Case/file number • Employee ID • Disability and medical information • Documentary evidence pertaining to Complainant, witnesses, or comparators,	**Specific PII identified in Section 4.2 that was acquired from this source (where relevant and necessary to investigating a claim):** Manager and witness PII collected is the same as for the complainant **with the following exceptions that are not collected** for managers or witnesses interviewed: • Personal email • Bargaining unit and union info • Medical information aside from disability description (not documentation) • Home address, telephone and fax • Personal cell phone • Protected genetic information • The Agency will generally provided documentary evidence pertaining to complainant, manager, or comparator employees including: • email chains • personnel documents (SF-50s, performance reviews, disciplinary letters, Etc.) • Settlement Agreement information • Unsworn testimonial statements by managers and witnesses

such as email chains and personnel documents (SF-50s, performance reviews, disciplinary letters, Etc.) • Settlement Agreement information • Unsworn testimonial statement by Complainant	
Manner in which information is acquired from source by the Treasury project/system: (select all that apply):	**Manner in which information is acquired from source by the Treasury project/system: (select all that apply):**
☒ From a paper or electronic form provided to individuals, the public or members of a particular group	☒ From a paper or electronic form provided to individuals, the public or members of a particular group
Please identify the form name (or description) and/or number (e.g., OMB Control Number): EEO Counseling Report and Individual Complaint of Employment Discrimination with the Department of the Treasury, TD F 62-03.5	Please identify the form name (or description) and/or number (e.g., OMB Control Number): EEO Counseling Report and Individual Complaint of Employment Discrimination with the Department of the Treasury, TD F 62-03.5
☒ Received in paper format other than a form.	☒ Received in paper format other than a form.
☐ Delivered to the project on disk or other portable device and uploaded to the system.	☒ Delivered to the project on disk or other portable device and uploaded to the system.
☐ Accessed and downloaded or otherwise acquired via the internet	☒ Accessed and downloaded or otherwise acquired via the internet
☒ Email	☒ Email
☒ Scanned documents uploaded to the system.	☒ Scanned documents uploaded to the system.
☐ Bulk transfer	☐ Bulk transfer
☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
☐ Fax	☐ Fax
☒ Extracted from notes of a phone interview or face to face contact	☒ Extracted from notes of a phone interview or face to face contact
☒ Other: Please describe: US mail, then scanned. .	☒ Other: Please describe: US Mail then scanned. _____

Section 4.4: Privacy and/or civil liberties risks related to collection

Notice of Authority, Principal Uses, Routine Uses, and Effect of not Providing Information

When Federal agencies use a form to obtain information from an individual that will be maintained in a system of records, they must inform the individual of the following: "(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on her/him, if any, of not providing all or any part of the requested information." 5 U.S.C § 522a(e)(3).

Section 4.4(a) ☒ Yes ☐ No Is any of the PII maintained in the system or by the project collected directly from an individual? **Section 4.4(b)** ☒ Yes ☐ No ☐ N/A Was the information collected from the individual using a form (paper or electronic)?

Section 4.4(c) ☒ Yes ☐ No ☐ N/A If the answer to Section 4.4(b) was "yes," was the individual notified (on the form in which the PII was collected or on a separate form that can be retained by the individual) about the following at the point where the information was collected (e.g., in a form; on a website).

☒ The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
☒ Whether disclosure of such information is mandatory or voluntary.
☒ The principal purpose or purposes for which the information is intended to be used.
☒ The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
☒ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

No privacy or civil liberties issues were identified because all of these requirements are metwith privacy act notifications that are included on each form and for each witness being asked to provide information: the Report of Counseling, the formal complaint form, and as a preamble to the individual affidavits.

Use of Social Security Numbers

Social Security numbers ("SSN") are commonly used by identity thieves to commit fraudulent acts against individuals. The SSN is one data element that has the ability to harm the individual and requires more protection when used. Therefore, and in an effort to reduce risk to individuals and federal agencies, OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, (May 22, 2007) required agencies to reduce the use of SSNs in agency systems and programs and to identify instances in which the collection is superfluous. In addition, OMB mandated agencies to explore alternatives to agency use of SSNs as personal identifiers for Federal employees and members of the public.

In addition, the Privacy Act provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *Id.* at § 7(a)(2)(A)-(B).

Section 4.4(d) ☐ Yes ☒ No ☐ N/A Does the system or project maintain SSNs?

Section 4.4(e) ☐ Yes ☐ No ☒ N/A Are there any alternatives to the SSNs as a personal identifier? If yes, please provide a narrative explaining why other alternatives to identify individuals will not be used. unique identifiers are used in place of SSNs.

Section 4.4(f) ☐ Yes ☐ No ☒ N/A Will individuals be denied any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN? If yes, please check the applicable box::

☐ SSN disclosure is required by Federal statute or Executive Order, or

☐ the SSN is disclosed to any Federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

Section 4.4 (g) Yes No N/A ☒ When the SSN is collected, are individuals given notice whether disclosure is mandatory or voluntary, the legal authority such number is solicited, and what uses will be made of it? If yes, please explain what means are used to provide notice.

No privacy and civil liberties issues were identified because SSNs are not collected. If SSNs are included in personnel or other documents that are deemed relevant and necessary, the SSNs are redacted before the document in which they are contained is uploaded to the system and included in the investigative file being issued.

First Amendment Activities

The Privacy Act provides that Federal agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

Section 4.4(h) ☒ Yes ☐ No Does the system or project maintain any information describing how an individual exercises their rights guaranteed by the First Amendment?

Section 4.4(h) If the system or project maintains information describing how an individual exercises their rights guaranteed by the First Amendment, do any of the following exceptions apply (the information may be maintained if any of the exceptions apply)?

☒ N/A (system or project does not maintain any information describing how an individual exercises their rights guaranteed by the First Amendment so no exceptions are needed)

☒ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.

☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity.

☒ There is a statute that expressly authorizes its collection.

As part of its mission, OCRD is required to counsel and receive discrimination complaints for administrative review from job applicants and federal employees. The allegations upon which an employee may seek counseling (and later file a complaint in some cases) could be based on discrimination because of the complainant's religion, or the Agency's refusal to provide a religious accommodation. In order to process these types of claims as required by law, OCRD must collect information that could, depending on the facts and circumstances of a particular case, be deemed to describe how an individual exercises rights guaranteed by the First Amendment (whether each collection meets the threshold requirements in Section (e)(7) of the Privacy Act depends on the circumstances and the jurisdiction in which a claim is brought; different federal courts apply different tests to determine whether the (e)(7) threshold is met). The individual also expressly consents to providing this information in order to pursue their complaint. Collection of some of this information is also authorized by title VII of the Civil Rights Act which expressly forbids discrimination based on religion (which must necessarily be collected in order to pursue such a

claim). Information regarding this type of allegation would be entered into the eComplaints site in the EEO Counseling form and the Individual Complaint of Employment Discrimination With the Department of the Treasury form, and would be developed in the investigative file.

Section 5: Maintenance, use, and sharing of the information

The following sections require a clear description of the system's or project's use of information.

Section 5.1: Describe how and why the system or project uses the information it collects and maintains

Please describe all of the uses of the information types and groupings collected and maintained by the system or project (see Section 4.2), including a discussion of why the information is used for this purpose and how it relates to the mission of the bureau or office that owns the system.

The information collected and maintained in the system is used to create and store a record for adjudication of EEO complaints filed by federal employees and job applicants. The adjudicating body could be the Department, the Equal Employment Opportunity Commission (EEOC), the Merit System Protections Board (MSPB), or a federal district court.

The PII in e-Complaints, e.g., names, position information, contact information, birth dates (month and year of birth only), demographic data, EEO case information, etc., is used to investigate and adjudicate formal complaints of discrimination for acts prohibited by EEO statutes (e.g., Title VII of the Civil Rights Act, the Age Discrimination in Employment Act (ADEA), Rehabilitation Act, etc.), regulations, and/or Executive Orders.

This usage is consistent with the EEOC's (and OCRD's) mission of rooting out prohibited discrimination because it allows OCRD to investigate complaints of discrimination for the Treasury's 12 Bureaus so that OCRD, EEOC and MSPB, as well as federal courts, may adjudicate complaints of discrimination and enforce compliance with orders of relief and Bureau settlement agreements.

Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them

The Privacy Act requires that Federal agencies "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." 5 U.S.C. § 552a(e)(2).

Section 5.1(a) ☒ Yes ☐ No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination about an individual's rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

Section 5.1(b) ☒ Yes ☐ No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual's rights, benefits, and privileges under federal programs?

Section 5.1(c) ☒ Yes ☐ No ☐ N/A If information could potentially be used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs, does the system or project collect

information (to the greatest extent practicable) directly from the individual?
The documents contained in the eComplaints system may be used to make adverse administrative determinations against the complaining employee/job applicant or the employer. Some of the information used to make these determinations is derived directly from the individuals about whom an adverse determination may be made. Other information may come from witnesses who are not parties to the EEO complaint, but who have knowledge regarding the claims. If the employee/applicant elects a hearing, an Administrative Judge (AJ) from the Equal Employment Opportunity Commission (EEOC) may schedule the complaint for a hearing. Either party to this proceeding may request that discovery be done if information is missing from the Investigative File. During the hearing, questions are asked under oath, and the proceedings are recorded by a court reporter who prepares a transcript for both parties. All parties are given an opportunity to rebut statements made by witnesses during this hearing. If a final agency decision (FAD) is issued, the individual may appeal the decision to the EEOC, the MSPB (if a "mixed case" that concerns an adverse action), or directly to federal court.

Data Mining

As required by Section 804 of the Implementing the 9/11 Commission Recommendations Act of 2007 ("9-11 Commission Act"), Treasury reports annually to Congress on its data mining activities. For a comprehensive overview of Treasury's data mining activities, please review the Department's Annual Privacy reports available at: http://www.treasury.gov/privacy/annual-reports.

Section 5.1(d) ☐ Yes ☒ No Is information maintained in the system or by the project used to conduct "data-mining" activities as that term is defined in the Implementing the 9-11 Commission Act?

Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared

Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

The Privacy Act requires that Federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C § 552a(e)(5). If a particular system of records meets certain requirements (including the NPRM process defined in Section 2 above), an agency may exempt the system of records (or a portion of the records) from this requirement.

Section 5.2(a) ☒ Yes ☐ No Is all or any portion of the information maintained in the system or by the project: (a) part of a system of records and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the Privacy Act?
Information in the eComplaints system may be used to make adverse determinations about the complainant or the agency/Bureau. In collecting information during an EEO investigation, it is often impossible or unfeasible to determine accuracy, relevance, timeliness, and completeness at the time the information is collected. Information that may initially appear accurate, relevant, timely and complete may, when analyzed with other available information (including information provided by the opposing party and non-party witnesses),be found to be inaccurate, irrelevant, untimely and incomplete as an investigation progresses. Complainants may provide information to supplement the Investigative File and may request a hearing (that allows for full exploration of

conflicting facts). These issues are addressed during the process and are generally captured in a final agency decision (FAD) or the EEOC hearing decision. so accuracy, relevance, timeliness, and completeness of information may be addressed as part of the FAD. Appeals processes also seek to ensure fairness to the individuals involved in the EEO process.so accuracy, relevance, timeliness, and completeness of information may be addressed as part of the FAD.

Computer Matching

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act imposing additional requirements when Privacy Act systems of records are used in computer matching programs.

Pursuant to the Privacy Act, as amended, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated systems of records or a system of records with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8).

Matching programs must be conducted pursuant to a matching agreement between the source and recipient agencies. The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

Section 5.2(b) ☐ Yes ☒ No Is any of the information maintained in the system or by the project (a) part of a system of records and (b) used as part of a matching program?
Section 5.2(c) ☐ Yes ☐ No ☒ N/A Is there a matching agreement in place that contains the information required by Section (o) of the Privacy Act?
Section 5.2(d) ☐ Yes ☐ No ☒ N/A Are assessments made regarding the accuracy of the records that will be used in the matching program?
Section 5.2(e) ☐ Yes ☐ No ☒ N/A Does the bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings, or obtain Data Integrity Board approval in accordance with Section (p) of the Privacy Act before taking adverse action against the individual?

Ensuring Fairness in Making Adverse Determinations About Individuals

Federal agencies are required to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5). This requirement also applies when merging records

from two or more sources where the merged records are used by the agency to make any determination about any individual.

Section 5.2(f) ☒ Yes ☐ No With respect to the information maintained in the system or by the project, are steps taken to ensure all information used to make a determination about an individual is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?
Information in the eComplaints system may be used to make adverse determinations about the complainant or the agency/Bureau. In collecting information during an EEO investigation, it is often impossible or unfeasible to determine accuracy, relevance, timeliness, and completeness at the time the information is collected. Information that may initially appear accurate, relevant, timely and complete may, when analyzed with other available information (including information provided by the opposing party and non-party witnesses), be found to be inaccurate, irrelevant, untimely and incomplete as an investigation progresses. Complainants may provide information to supplement the Investigative File and may request a hearing (that allows for full exploration of conflicting facts). These issues are addressed during the process and are generally captured in a final agency decision (FAD) or the EEOC hearing decision.. so accuracy, relevance, timeliness, and completeness of information may be addressed as part of the FAD. Appeals processes also seek to ensure fairness to the individuals involved in the EEO process.

Merging Information About Individuals

Section 5.2(g) ☐ Yes ☒ No Is information maintained in the system or by the project merged with electronic or non-electronic information from internal or external sources (e.g., other files or systems)? **Section 5.2(h)** ☐ Yes ☐ No ☒ N/A Once merged, is the information used in making determinations about individuals (e.g., decisions about whether the individual will receive a financial benefit or payment, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)? **Section 5.2(i)** ☐ Yes ☐ No ☒ N/A Are there documented policies or procedures for how information is merged? **Section 5.2(j)** ☐ Yes ☐ No ☒ N/A Do the documented policies or procedures address how to proceed when partial matches (where some, but not all of the information being merged matches a particular individual) are discovered after the information is merged? **Section 5.2(k)** ☐ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make a determination about an individual, are steps taken to ensure the accuracy, relevance, timeliness, and completeness of the information as is reasonably necessary to assure fairness to the individual?
Information maintained in the system or by the project is not merged with electronic or non-electronic information from internal or external sources. Therefore, no privacy and civil liberties risks were identified.

Policies and Standard Operating Procedures or Technical Solutions Designed to Ensure Information Accuracy, Completeness, and Timeliness

Section 5.2(l) ☒ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make any determination about an individual (even if it is an exempt system of records), are there documented policies or standard operating procedures for the system or project that address the accuracy, completeness, and timeliness of the information? **Section 5.2(m)** ☒ Yes ☐ No Does the system or project use any software or other technical solutions designed to improve the accuracy, completeness, and timeliness of the information used to make an adverse determination about an individual's rights, benefits, and/or privileges (regardless of if it is an exempt system of records)?
Information in the eComplaints system may be used to make adverse determinations about the complainant or the agency/Bureau. In collecting information during an EEO investigation, it is often impossible or unfeasible

to determine accuracy, relevance, timeliness, and completeness at the time the information is collected. Information that may initially appear accurate, relevant, timely and complete may, when analyzed with other available information (including information provided by the opposing party and non-party witnesses), be found to be inaccurate, irrelevant, untimely and incomplete as an investigation progresses. Complainants may provide information to supplement the Investigative File and may request a hearing (that allows for full exploration of conflicting facts). These issues are addressed during the process and are generally captured in a final agency decision (FAD) or the EEOC hearing decision.. so accuracy, relevance, timeliness, and completeness of information may be addressed as part of the FAD. Appeals processes also seek to ensure fairness to the individuals involved in the EEO process.

Accuracy, Completeness, and Timeliness of Information Received from the Source

Section 5.2(n) ☒ Yes ☐ No Did Treasury or the bureau receive any guarantee, assurance, or other information from any information source(s) regarding the accuracy, timeliness and completeness of the information maintained in the system or by the project?

To some extent, all parties and witnesses in administrative EEO proceedings assert the accuracy, timeliness and completeness of the information they provide. For example, affidavits are signed under penalty of perjury. Due process is provided during the proceedings because determinations are made by neutral Administrative Judges who test the credibility and quality of the information provided in making a determination. If a party disagrees with that outcome, an appeals process is available. Regulations and policies also work to ensure accuracy, completeness, and timelines. These include the EEOC Regulations at 29 CFR Part 1614, which set regulatory time frames for the different stages of the process (e.g., 180 days to complete an investigation), internal office SOPs, EEOC Management Directive 110, iComplaints business rules (iComplaints is an online application for tracking case information).

Disseminating Notice of Corrections of or Amendments to PII

Section 5.2(o) ☐ Yes ☒ No ☐ N/A Where feasible and appropriate, is there a process in place for disseminating corrections of or amendments to the PII maintained in the system or by the project to all internal and external information-sharing partners?

Section 5.2(p) ☐ Yes ☒ No ☐ N/A Where feasible and appropriate, does the process for disseminating corrections or amendments include notifying the individual whose information is corrected or amended?

The proceedings are designed to determine which parties' information is correct. It would defeat the purpose of the proceedings to correct statements made by either party in the record (except in the final agency decision). Doing so would have an adverse effect on the the fairness of any appeal that allows appellate reconsideration of the quality and legal sufficiency of statements the parties and witnesses made previously in support of their claims and defenses.

Section 5.3: Information sharing within the Department of the Treasury

Internal Information Sharing

Section 5.3(a) ☒ Yes ☐ No Is PII maintained in the system or by the project shared with other Treasury bureaus?

Section 5.3(b) ☒ Yes ☐ No ☐ N/A Does the Treasury bureau or office that receives the PII limit access to those Treasury officers and employees who have a need for the PII in the performance of their official duties (i.e., those who have a "need to know")?

OCRD forwards case documents and files to the particular Bureau from which the complaint arose. The Bureaus cannot actually access the eComplaints system to search for files, but they receive a link to download case documents and files for a certain period of time before the link expires. The link may only be accessed by the addressee, who is generally the EEO Officer or someone acting for the EEO Officer; it cannot be forwarded to others. If a complainant elects a hearing or appeals a final agency decision, the case file may be forwarded to the Bureau's Counsel's office.

Memorandum of Understanding/Other Agreements Limiting Treasury's Internal Use/Disclosure of PII
Section 5.3(c) ☐ Yes ☒ No ☐ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency that provided the information to the Treasury or subject to an international agreement or treaty) that limits or places conditions on Treasury's internal use, maintenance, handling, or disclosure of the PII?
There is no agreement that places restrictions on OCRD's use, maintenance, handling, or disclosure of the PII (though OCRD imposes its own restrictions).

Internal Information Sharing Chart	
Internal Recipient's Name (e.g., bureau or office)	*All Bureaus – EEO Offices and General Counsel offices*
Purpose of the Sharing	Bureau EEO Offices are co-custodians of the files for their Bureau; we also send the files to Counsels offices to prepare for hearing or appeals
PII Shared	Same as listed above under 4.3
Applicable Statutory or Regulatory or Restrictions on Information Shared	The two conditions most likely to apply in the context of an agency's EEO program are: 1) disclosure to employees of the agency where the EEO file is kept, who have a need for the file information in the performance of their duties; and 2) disclosure permitted under certain published "routine uses."
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	N/A
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling, or Sharing of PII Received	N/A
Method of PII Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/other (please describe if other)	Email link to downloadable documents using eComplaints; Email to Treasury employee email addresses.
The Bureau EEO Offices are co-custodians of the EEO complaint files of their employees. OCRD copies Bureau EEO Offices on all investigatory files being issued for employees of their Bureau. Counsel will receive a copy of the complaint files when an employee of their Bureau requests a hearing or appeals a decision.	

Section 5.4: Information sharing with external (i.e., outside Treasury) organizations and individuals

External Information Sharing
Section 5.4(a) ☒ Yes ☐ No Is PII maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?
Complaint files are sent to the EEOC if a hearing is requested or an appeal is filed. If the complainant elects an MSPB or federal court hearing, Counsel (not OCRD) will generally provide the case files in those forums. *Affidavits contain the following notice to complainants and witnesses with regard to information sharing:*

The information you supply will be used along with data you supplied previously and information developed by investigation to resolve your EEO complaint. This information may be furnished to designated officers, employees and contractors of the Department of the Treasury, the Equal Employment Opportunity Commission (EEOC) or the Merit Systems Protection Board in order to resolve your EEO complaint. The information may also be disclosed to another federal agency, to a court, or to a party in litigation before a court or in an administrative proceeding when the government is a party and the information is relevant to the subject matter of the proceeding; to a congressional office at your request; to a duly authorized official engaged in investigation or settlement of a grievance, complaint or appeal filed by an employee; to officials of state or local bar associations or disciplinary boards or committees when they are investigating complaints against attorneys; or to a federal agency in response to a request for information in connection with the hiring of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, or the lawful statutory, administrative, or investigative purpose of the agency.

The EEOC SORN GOVT-1 lists the routine uses of records maintained in the system as quoted below. These records and information in these records may be used:

a. *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.*
b. *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 government is a party to the judicial or administrative proceeding.*
c. *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.*
d. *To disclose to an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint or appeal filed by an employee.*
e. *To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.*
f. *To disclose information to officials of state or local bar associations or disciplinary boards or committees when they are investigating complaints against attorneys in connection with their representation of a party before EEOC.*
g. *To disclose to a Federal agency in the executive, legislative, or judicial branch of government, in response to its request information in connection with the hiring of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision.*
h. *To disclose information to employees of contractors engaged by an agency to carry out the agency's responsibilities under 29 CFR part 1614.*
i. *To disclose information to potential witnesses as appropriate and necessary to perform the agency's functions under 29 CFR part 1614.*

Accounting of Disclosures

Section 5.4(b) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, do you maintain a paper or electronic log or other record of the date, nature, and purpose of each disclosure (not including intra-agency disclosures and FOIA disclosures) of a record to any person or to another agency (outside of Treasury) and the name and address of the person or agency to whom the disclosure is made?

Section 5.4(c) ☒ Yes ☐ No ☐ N/A If you do not keep a running tabulation of every disclosure at the time it is made, are you able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to Privacy Act requests in a timely fashion?

Section 5.4(d) ☒ Yes ☐ No ☐ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, do you retain the log or other record of the date, nature, and purpose of each disclosure, for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made?

Section 5.4(e) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to make the accounting available to the individual named in the record?

Section 5.4(f) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to inform any person or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made?

The sharing of complaint files or information with indivduals or organizations outside of Treasury generally occurs in the context of completing EEO complaint investigations or in forwarding complaint files for hearings or appeals with EEOC, MSPB, or in federal court. The complainants are notified of external disclosures with respect to EEO investigations because they receive a copy of the investigatory file. Complainants are also notified when a disclosure is made to adjudicating bodies because the complainant must be copied on all hearing or appeal correspondence to preserve impartiality.

Statutory or Regulatory Restrictions on Disclosure

Section 5.4(g) ☒ Yes ☐ No In addition to the Privacy Act, are there any other statutory or regulatory restrictions on the sharing of any of the PII maintained in the system or by the project (e.g., 26 U.S.C § 6103 for tax returns and return information)?

The EEOC promulgated a regulation that governs all records contained in system EEOC/GOVT-1, including those maintained by Treasury and other federal agencies. 29 CFR Part 1611. Requests for access to, an accounting of disclosures for, or amendment of records covered by the EEOC/GOVT-1 systems of records notice must be processed by agency personnel in accordance with this regulation.

Memorandum of Understanding Related to External Sharing

Section 5.4(h) ☐ Yes ☒ No ☐ N/A Has Treasury (including bureaus and offices) executed a Memorandum of Understanding, or entered into any other type of agreement, with any external agencies, organizations, or individuals with which/whom it shares PII maintained in the system or by the project?

There is an Interagency Agreement in place between Treasury and USPS that was signed in August 2014, which delineates the contractual relationship between the agencies for the purpose of obtaining EEO complaint services (thus far limited to investigations) from USPS.

Memorandum of Understanding Limiting Treasury's Use or Disclosure of PII

Section 5.4(i) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency, an international agreement or treaty, or contract with private vendor that provided the information to Treasury or one of its bureaus) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII?

The above-mentioned Treasury-USPS IAA requires adherence to "Federal laws, regulations, and rules

regarding the confidentiality of EEO records . . . .” i.e., the requirements are the same as those that OCRD must abide by in using and disclosing PII as delineated by the Privacy Act and the EEOC regulations implementing the Act. 29 C.F.R. Part 1611.

Memorandum of Understanding Limiting External Party's Use or Disclosure of PII

Section 5.4(j) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party's use, maintenance, handling, or disclosure of PII shared by Treasury?

The above-mentioned Treasury-USPS IAA requires adherence to “Federal laws, regulations, and rules regarding the confidentiality of EEO records . . . .” i.e., the requirements are the same as those that OCRD must abide by in using and disclosing PII as delineated by the Privacy Act and the EEOC regulations implementing the Act. 29 C.F.R. Part 1611. Other adjudicatory bodies that receive complaint information (EEOC, MSPB, federal courts) are subject ot the same statutory Privacy Act restrictions on the use of EEO complaint information.

External Information Sharing Chart

Section 5.4(k) ☒ Yes ☐ No Is information from the system or project shared externally? *o*

External Recipient's Name	**EEOC/MSPB**	**Witnesses Outside of Treasury employment**	**Congressional inquiry**	**FOIA response to an individual outside Treasury**
Purpose of the Sharing PII Shared	Resolution of EEO complaint	To obtain additional relevant testimony for the record to support or contradict the complainant's contentions	To respond to Congressional inquiry into an EEO matter	To respond to a FOIA request
Content of Applicable Routine Use/Citation to the SORN	GOVT-1, d. To disclose to an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint or appeal filed by an employee.	GOVT-1, e. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding. i. To disclose information to potential witnesses as appropriate and necessary to perform the agency's functions under 29 CFR part	GOVT-1, c. 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.	Required by the Freedom of Information Act, 5 USC 552.

		1614.		
Applicable Statutory or Regulatory or Restrictions on Information Shared	5 U.S.C. 552a	5 U.S.C. 552a	5 U.S.C. 552a	5 U.S.C. 552a
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Source/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A	N/A	N/A	N/A
Name and Description of Relevant MOUs or Other Agreements Containing Restrictions Imposed by Treasury on External Sharing Partner (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A	N/A	N/A	N/A
Method(s) Used to Transfer PII (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other)	Electronic upload to EEOC secure web application FedSep.; paper and CD sent via US mail	paper and/or CD sent via US mail with interrogatories.	paper and/or CD sent via US mail.	paper and/or CD sent via US mail.

External Disclosures (cont'd)

External Recipient's Name	**USPS/Investigator**	**District Court**
Purpose of the Sharing PII Shared	Resolution of EEO complaint requires creating a factual record.	Resolution of EEO complaint.
Content of Applicable Routine Use/Citation to the SORN	GOVT-1 h. To disclose information to	GOVT-1 b. To disclose information to another

	employees of contractors engaged by an agency to carry out the agency's responsibilities under 29 CFR part 1614.	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 government is a party to the judicial or administrative proceeding.
Applicable Statutory or Regulatory or Restrictions on Information Shared	5 U.S.C. 552a	5 U.S.C. 552a
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Source/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A	N/A
Name and Description of Relevant MOUs or Other Agreements Containing Restrictions Imposed by Treasury on External Sharing Partner (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A	N/A
Method(s) Used to Transfer PII (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other)	Encrypted email to .gov emails via Outlook.	paper and/or CD sent via US mail

Obtaining Consent Prior to New Disclosures Not Included in the SORN or Authorized by the Privacy Act
Section 5.4(l) ☐ Yes ☐ No ☒ N/A Is the individual's consent obtained, where feasible and appropriate, prior to any **new** disclosures of previously collected records in a system of records (those not expressly authorized by the Privacy Act or contained in the published SORN (e.g., in the routine uses))?
No external disclosures of the information are made without notice to the parties. The disclosures are required by law so consent is unnecessary.

Section 6: Compliance with federal information management requirements

Responses to the questions below address the practical, policy, and legal consequences of failing to comply with one or more of the following federal information management requirements (to the extent required) and how those risks were or are being mitigated: (1) the

Privacy Act System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Gov Act security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

Section 6.1: Privacy Act System of Records Notice (SORN)

For collections of PII that meet certain requirements, the Privacy Act requires that the agency publish a SORN in the *Federal Register*.

System of Records
Section 6.1(a) ☒ Yes ☐ No Does the system or project retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? **Section 6.1(b)** ☒ Yes ☐ No ☐ N/A Was a SORN published in the *Federal Register* for this system of records?
Systems of Records Notices: • EEOC/GOVT-1 (July 30, 2002, 67 FR 49338) • Treasury .013-Department of the Treasury Civil Rights Complaints and Compliance Review Files (January 2, 2014, 79 FR 183) • Treasury/IRS 00.001 - Correspondence Files (including Stakeholder Relationship • files and Correspondence Control Files) • Treasury/IRS 34.037 - IRS Audit Trail and Security Records System • Treasury/IRS 00.007 Employee Complaints and Allegation Referral Records

Section 6.2: The Paperwork Reduction Act

The PRA requires OMB approval before a Federal agency may collect standardized data from 10 or more respondents within a 12 month period. OMB requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

Paperwork Reduction Act Compliance
Section 6.2(a) ☒ Yes ☐ No Does the system or project maintain information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government)? **Section 6.2(b)** ☒ Yes ☐ No ☐ N/A Does the project or system involve a new collection of information in identifiable form for 10 or more persons from outside the federal government? **Section 6.2(c)** ☐ Yes ☒ No ☐ N/A Did the project or system complete an Information Collection Request ("ICR") and receive OMB approval?
OCRD is in the process of developing a single departmentwide EEO complaint form to replace the preexisting individual forms used by each bureau. Once OCRD obtains concurrence on a single, internal form for all of Treasury, OCRD will work with the DO PRA Specialist to complete the necessary documents to obtain OMB approval of (and an OMB Control Number for) the departmentwide form.

Section 6.3: Records Management - NARA/Federal Records Act Requirements

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the NARA for permanent retention upon expiration of this period.

NARA Records Retention Requirements
Section 6.3(a) ☒ Yes ☐ No Are the records used in the system or by the project covered by NARA's General Records Schedules ("GRS") or Treasury/bureau Specific Records Schedule (SRS)? **Section 6.3(b)** ☒ Yes ☐ No Did NARA approved a retention schedule for the records maintained in the system or by the project? **Section 6.3(c)** ☐ Yes ☐ No ☒ N/A If NARA did not approve a retention schedule for the records maintained in the system or by the project and the records are not covered by NARA's GRS or Treasury/bureau SRS, has a draft retention schedule (approved by all applicable Treasury and/or Bureau officials) been developed for the records used in this project or system?
The records are covered by GRS 1, Civilian Personnel Records (Transmittal No. 24, August 2015) (number 25 deals with EEO Records).

Section 6.4: E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act ("FISMA") Security Assessment & Authorization (SA&A) process is required before a federal information system may receive Authority to Operate ("ATO"). Different security requirements apply to National Security Systems.

Federal Information System Subject to FISMA Security Assessment and Authorization
Section 6.4(a) ☒ Yes ☐ No ☐ N/A Is the system a federal information system subject to FISMA requirements? **Section 6.4(b)** ☒ Yes ☐ No ☐ N/A Has the system or project undergone a SA&A and received ATO?
The ECM Platform is currently undergoing a new SA&A.ECM has an ATO and is currently undergoing a new SA&A that is due to be complete by the end of July 2016.
Access Controls and Security Requirements
Section 6.4(c) ☒ Yes ☐ No Does the system or project include access controls to ensure limited access to information maintained by the system or project?
Only OCRD staff may access the site itself. The System Owner can add users, and assign permissions and roles for OCRD staff to access the site. Files may be forwarded via a link to authorized Department staff outside of OCRD (Bureau EEO and Counsel) but these individuals cannot access the actual site, only the links forwarded that open up the document(s) on a unique ECM site with only the select document(s) for download. We are in process of limiting the Outlook address book so that only authorized personnel are listed for selection to receive links to download EEO files – to minimize the risk of selecting the wrong person in the Outlook "people picker."
Security Risks in Manner of Collection
Section 6.4(d) ☒ Yes ☐ No In Section 4.3 above, you identified the sources for information used in the system or project and the method and manner of collection. Were any security, privacy, or civil liberties risks identified with respect to the manner in which the information is collected from the source(s)?
The Report of Counseling is received via download from a secure online system (iComplaints) that is accessed only by OCRD and Bureau EEO Offices. Complaint forms are received via US mail, or email to an office complaints mailbox EEOComplaints@treasury.gov. We are currently waiting on the implementation of a 2016 task order to require complainants who wish to submit formal complaints electronically, to direct submission only via a secure upload to a public-facing Treasury website that uses a captcha upon transmission, that will send the complaint documentation to our email box – rather than the current method of using submission via personal email, as currently stands. When corresponding with complainants who are not employed by

Treasury or who do not wish to use their Treasury secure email, we generally use US mail. USPS contractor investigators must use US mail or a secure federal .gov email for transmitting EEO complaint information. EEO investigative files are sent from USPS to OCRD in hard copy and CD format via US main, then uploaded to eComplaints.

Security Controls When Sharing Internally or Externally
Section 6.4(e) ☒ Yes ☐ No ☐ N/A Are all Treasury/bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system to internal or external parties?
Only authorized OCRD staff can view the files in the E-complaints system. When sharing with Counsel or EEO Officers, we generally share a link to a downloadable file that expires after 60 days. These links when forwarded will not open; they only open for the individual user to whom the link was sent. Files shared with EEOC are uploaded to their secure application FedSep. Files sent to complainants and their reps are sent via US mail and occasionally via secure email within the Treasury system (for current employees of Treasury).

Monitoring of Individuals
Section 6.4(f) ☒ Yes ☐ No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?
eComplaints users are monitored only with respect to their use of the system. Audit logs are maintained to ensure access is to particular files is limited to individualsd who have a need to know that information in order to perform their official duties.

Audit Trails
Section 6.4(g) ☒ Yes ☐ No Are audit trails regularly reviewed for appropriate use, handling, and disclosure of PII maintained in the system or by the project inside or outside of the Department?
Audit logs are regularly monitored in accordance with Treasury OCIO requirements.

Section 6.5: Section 508 of the Rehabilitation Act of 1973

When Federal agencies develop, procure, maintain, or use Electronic and Information Technology ("EIT"), Section 508 of the Rehabilitation Act of 1973 (as amended in 1998) requires that individuals with disabilities (including federal employees) must have access and use (including privacy policies and directives as well as redress opportunities) that is comparable to that which is available to individuals who do not have disabilities.

Applicability of and Compliance With the Rehabilitation Act
Section 6.5(a) ☒ Yes ☐ No Will the project or system involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)?
Section 6.5(b) ☒ Yes ☐ No ☐ N/A Does the system or project comply with all Section 508 requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities?
No privacy and civil liberties issues were identified because the system is in compliance with Section 508.

Section 7: Redress

Access Under the Freedom of Information Act and Privacy Act
Section 7.0(a) ☒ Yes ☐ No Does the agency have a published process in place by which individuals may seek records under the Freedom of Information Act and Privacy Act?
The Treasury/bureaus FOIA and Privacy Act disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C.

Under 29 CFR § 1611.13(f), the EEOC determined that EEO complaint files covered by GOVT-1 are exempt from subsections (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) of the Privacy Act as necessary for the agency's law enforcement efforts.

Privacy Act Access Exemption

Section 7.0(b) ☐ Yes ☒ No Was any of the information that is maintained in system of records and used in the system or project exempted from the access provisions of the Privacy Act?

Additional Redress Mechanisms

Section 7.0(c) ☐ Yes ☒ No With respect to information maintained by the project or system (whether or not it is covered by the Privacy Act), does the bureau or office that owns the project or system have any additional mechanisms other than Privacy Act and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

The EEO process contains its own, built-in redress opportunities. Depending on the type of employment action at issue, Complainants will have a right to appeal the final agency decision to either the EEOC or MSPB within 30 days, as well as to federal district court.

Responsible Official

Timothy H. Skinner
Privacy and Civil Liberties Officer
Departmental Offices
U.S. Department of the Treasury

Approval Signature

Timothy Skinner

Digitally signed by Timothy Skinner
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Departmental Offices, ou=People, serialNumber=656801, cn=Timothy Skinner
Date: 2016.07.15 15:57:13 -04'00'

Timothy H. Skinner
Director, Privacy and Civil Liberties
Office of Privacy, Transparency, & Records
Department of the Treasury