



Privacy and Civil Liberties Impact Assessment
for the
Treasury iComplaints EEO Case Management System

July 15, 2016

Reviewing and Certifying Official
Timothy H. Skinner
Director, Privacy and Civil Liberties
Office of Privacy, Transparency & Records
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. PCLIA’s 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 iComplaints system was previously housed at the IRS (under the name I-Trak) which did a Privacy Impact Assessment on the system at that time. This is the first time Treasury DO has completed a PCLIA for the system under its new name, iComplaints.

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 limited 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 PCLIA 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

iComplaints is one of two systems used to process EEO counseling consultations and case information. The purpose of the Treasury iComplaints system is to process, manage, and report information related to administrative, departmentwide EEO cases as well as to provide aggregate EEO data for internal reports (including the form 462 “Report to the Equal Employment Opportunity Commission (EEOC)”). iComplaints also maintains reports from EEO counseling sessions, acceptance letters (wherein the agency acknowledges it has accepted claims outlined in a formal EEO complaint) and Final Agency Decisions (FAD) (if one is issued). Participation in an informal/counseling stage is a prerequisite for 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, The Office of Civil Rights and Diversity (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 and 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 conducting a separate PCLIA. The iComplaints system significantly reduces the amount of paper processing of complaints and allows the Department to have the most up to date case processing data in real time.

eComplaints (the subject of a separate PCLIA) is the system used to adjudicate EEO complaints. The EEO Report of Counseling, acceptance letters, report of investigation, correspondence, and FAD (where applicable) are uploaded into the eComplaints system to allow EEO case specialists to determine the viability of EEO complaints.

Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project		
<input type="checkbox"/> 0 – 999	<input checked="" type="checkbox"/> 1000 – 9,999	<input type="checkbox"/> 10,000 – 99,999
<input type="checkbox"/> 100,000 – 499,999	<input type="checkbox"/> 500,000 – 999,999	<input type="checkbox"/> 1,000,000+

Section 3.2: Authority to Collect

The authority for operating this system is found in: 29 CFR Part 1614 subpart F, which directs and authorizes the Department to establish a system to collect and maintain accurate employment information

on the race, national origin, sex and disability of its employees and report to the EEOC information concerning pre-complaint counseling and the status, processing and disposition of complaints.

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 conditions 5 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.

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

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

- None of the [PII](#) maintained in the system or by the project is part of a [Privacy Act system of records](#);
- 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;
- 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;
- 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
- 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?

OCRCD only maintains Privacy Act records in the iComplaints system that are relevant and necessary to the EEO mission. This is achieved by using forms that contain questions that are narrowly tailored to obtain information necessary to the completion of a "Report of Counseling" form. Final agency decisions (FADs), are final decisions issued by the agency. FADs are also narrowly tailored to contain only information relevant and necessary to resolving the factual and legal issues presented in the case. The remainder of the information in the system is tracking information that is also narrowly tailored to information needed to meet EEOC and other reporting requirements.

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.

Please select the appropriate boxes below to identify the types or groupings of information collected by the system or project. If the system or project uses groupings or information that are not listed below, please add them using the additional spaces provided.

Biographical/General Information		
<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Gender	<input type="checkbox"/> Group/Organization Membership
<input checked="" type="checkbox"/> Date of Birth	<input checked="" type="checkbox"/> Race	<input type="checkbox"/> Military Service Information
<input checked="" type="checkbox"/> Home Physical/Postal Mailing Address	<input checked="" type="checkbox"/> Ethnicity	<input checked="" type="checkbox"/> Personal Home Phone or Fax Number
<input checked="" type="checkbox"/> Zip Code	<input type="checkbox"/> Personal Cell Number	<input type="checkbox"/> Alias (including nickname)
<input type="checkbox"/> Business Physical/Postal Mailing Address	<input checked="" type="checkbox"/> Business Cell Number	<input type="checkbox"/> Business Phone or Fax Number
<input type="checkbox"/> Personal e-mail address	<input type="checkbox"/> Nationality	<input type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Business e-mail address	<input type="checkbox"/> Country of Birth	<input type="checkbox"/> Spouse Information
<input type="checkbox"/> Personal Financial Information (including loan information)	<input type="checkbox"/> City or County of Birth	<input type="checkbox"/> Children Information
<input type="checkbox"/> Business Financial Information (including loan information)	<input type="checkbox"/> Immigration Status	<input type="checkbox"/> Information about other relatives.
<input checked="" type="checkbox"/> Marital Status	<input type="checkbox"/> Citizenship	<input type="checkbox"/> Professional/personal references or other information about an individual's friends, associates or acquaintances.
<input checked="" type="checkbox"/> Religion/Religious Preference	<input type="checkbox"/> Device settings or preferences (e.g., security level, sharing options, ringtones).	<input type="checkbox"/> Global Positioning System (GPS)/Location Data
<input checked="" type="checkbox"/> Sexual Orientation	<input type="checkbox"/> User names, avatars etc.	<input type="checkbox"/> Secure Digital (SD) Card or Other Data stored on a card or other technology
<input type="checkbox"/> Cell tower records (e.g., logs, user location, time etc.)	<input type="checkbox"/> Network communications data	<input type="checkbox"/> Cubical or office number
<input type="checkbox"/> Contact lists and directories (known to contain personal	<input type="checkbox"/> Contact lists and directories (not known to contain personal	<input type="checkbox"/> Contact lists and directories (known to contain only business

information)	information, but uncertain)	information)
<input type="checkbox"/> Education Information	<input type="checkbox"/> Resume or curriculum vitae	<input checked="" type="checkbox"/> EEO Counselor Name
<input type="checkbox"/> Complainant's signature.	<input checked="" type="checkbox"/> Complainant's national origin.	<input checked="" type="checkbox"/> Name of applicant for a Treasury position: _____
<input checked="" type="checkbox"/> Name of Complainant's Representative.	<input checked="" type="checkbox"/> Counselor's signature	

Identifying Numbers	
<input type="checkbox"/> Full Social Security number	<input type="checkbox"/> Health Plan Beneficiary Number
<input type="checkbox"/> Truncated/Partial Social Security number (e.g., last 4 digits)	<input type="checkbox"/> Alien Registration Number
<input type="checkbox"/> Personal Taxpayer Identification Number	<input type="checkbox"/> Business Taxpayer Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Credit Card Number	<input type="checkbox"/> Business Credit Card Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Vehicle Identification Number	<input type="checkbox"/> Business Vehicle Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal License Plate Number	<input type="checkbox"/> Business License Plate Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input checked="" type="checkbox"/> File/Case ID Number (individual)	<input type="checkbox"/> File/Case ID Number (business) (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Professional License Number	<input type="checkbox"/> Business Professional License Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input checked="" type="checkbox"/> Employee Identification Number	<input type="checkbox"/> Patient ID Number
<input type="checkbox"/> Business Bank Account Number	<input type="checkbox"/> Personal Bank Account Number
<input type="checkbox"/> Commercially obtained internet navigation/purchasing habits of individuals	<input type="checkbox"/> Government obtained internet navigation/purchasing habits of individuals
<input type="checkbox"/> Business License Plate Number (non-sole-proprietor)	<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Personal device identifiers or serial numbers	<input type="checkbox"/> Other Identifying Numbers (please describe): _____
<input type="checkbox"/> 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)	<input type="checkbox"/> Other Identifying Numbers (please describe): _____

Medical/Emergency Information Regarding Individuals		
<input checked="" type="checkbox"/> Medical/Health Information	<input type="checkbox"/> Worker's Compensation Act Information	<input type="checkbox"/> Patient ID Number
<input type="checkbox"/> Mental Health Information	<input checked="" type="checkbox"/> Disability Information	<input type="checkbox"/> Emergency Contact Information (e.g., a third party to contact in case of emergency)
<input type="checkbox"/> 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		
<input checked="" type="checkbox"/> Physical description/	<input checked="" type="checkbox"/> Signatures (complainant,	<input type="checkbox"/> Vascular scans

characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) (only gender is collected in iComplaints where applicable)	complainant's representative and counselor)	
<input type="checkbox"/> Fingerprints	<input type="checkbox"/> Photos	<input type="checkbox"/> Retina/Iris Scans
<input type="checkbox"/> Palm prints	<input type="checkbox"/> Video	<input type="checkbox"/> Dental Profile
<input type="checkbox"/> Voice audio recording	<input type="checkbox"/> Scars, marks, tattoos	<input type="checkbox"/> DNA Sample or Profile
<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):

Specific Information/File Types		
<input type="checkbox"/> Taxpayer Information/Tax Return Information	<input type="checkbox"/> Law Enforcement Information	<input type="checkbox"/> Security Clearance/Background Check Information
<input type="checkbox"/> Civil/Criminal History Information/Police Records (government source)	<input type="checkbox"/> Credit History Information (government source)	<input type="checkbox"/> Bank Secrecy Act Information
<input type="checkbox"/> Civil/Criminal History Information/Police Records (commercial source)	<input type="checkbox"/> Credit History Information (commercial source)	<input type="checkbox"/> National Security/Classified Information
<input type="checkbox"/> Protected Information (as defined in Treasury Directive 25-10)	<input type="checkbox"/> Case files	<input type="checkbox"/> Personnel Files
<input type="checkbox"/> Information provided under a confidentiality agreement	<input type="checkbox"/> Information subject to the terms of an international or other agreement	<input checked="" type="checkbox"/> Other (please describe): The report of EEO counseling, the acceptance letter (wherein the agency states the claims asserted that must be investigated), and any final agency decision (FAD) issued.

Audit Log and Security Monitoring Information		
<input checked="" type="checkbox"/> User ID assigned to or generated by a user of Treasury IT	<input type="checkbox"/> Date and time an individual accesses a facility, system, or other IT	<input type="checkbox"/> Files accessed by a user of Treasury IT (e.g., web navigation habits)
<input type="checkbox"/> Passwords generated by or assigned to a user of Treasury IT	<input checked="" type="checkbox"/> Internet or other queries run by a user of Treasury IT	<input type="checkbox"/> Contents of files accessed by a user of Treasury IT
<input type="checkbox"/> Biometric information used to access Treasury facilities or IT	<input type="checkbox"/> Video of individuals derived from security cameras	<input type="checkbox"/> Public Key Information (PKI).
<input type="checkbox"/> 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	<input type="checkbox"/> Still photos of individuals derived from security cameras.	<input checked="" type="checkbox"/> Internet Protocol (IP) Address
<input checked="" type="checkbox"/> Other (please describe): Actions (password changes, log onto system), Description of action (successful or unsuccessful), URL, Date and Time Stamps, all uses of DBQ-SQL, system administrators actions. Audit trail assures only those with permission via	<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):

assigned roles can view and use iComplaints.		
--	--	--

Other	
<input type="checkbox"/> Other (please describe: _____)	<input type="checkbox"/> Other (please describe: _____)
<input type="checkbox"/> Other (please describe: _____)	<input type="checkbox"/> Other (please describe: _____)

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

In the boxes provided below, please list the sources for each personal identifier or grouping identified in Section 4.2 above. One chart must be filled out for each source. Please add columns as necessary.

The Individual Who Files an EEO Complaint or Seeks Counseling	The Employer About Whom a Complaint was Filed or About Whose Alleged Conduct an Employee Seeks Counseling
<p>Specific <u>PII</u> identified in Section 4.2 that was acquired from this source:</p> <p>Name (First, MI, Last) Employee ID from HRConnect Date of Birth Pay Plan Grade Series Race Ethnicity Gender Employee Type Occupation Work email Country Bargaining Unit Union Code Union Code Translation Disability Description Org. Code Home Address City/State/Zip Home Telephone Home Fax Personal Cell Phone Work Address Work City/State/Zip Work Telephone Work Fax Work Cell</p>	<p>Specific <u>PII</u> identified in Section 4.2 that was acquired from this source: Identifying Numbers</p> <p>Employee ID from HRConnect Date of Birth Pay Plan Grade Series Occupation Work email Country Bargaining Unit Union Code Union Code Translation Disability Description Org. Code Home Address City/State/Zip Home Telephone Home Fax Personal Cell Phone Work Address Work City/State/Zip Work Telephone Work Fax Work Cell</p>
<p>Manner in which information is acquired from source by the Treasury project/system: (select</p>	<p>Manner in which information is acquired from source by the Treasury project/system: (select</p>

all that apply):	all that apply):
<input checked="" type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input checked="" type="checkbox"/> 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- Individual Complaint, TD F 62-03.1 & 62-03.1a 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- Individual Complaint, TD F 62-03.1a and Individual Complaint of Employment Discrimination with the Department of the Treasury, TD F 62-03.5
<input type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.
<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.
<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet
<input type="checkbox"/> Email	<input type="checkbox"/> Email
<input type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.
<input type="checkbox"/> Bulk transfer	<input type="checkbox"/> Bulk transfer
<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
<input type="checkbox"/> Fax	<input type="checkbox"/> Fax
<input checked="" type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input checked="" type="checkbox"/> Extracted from notes of a phone interview or face to face contact
<input checked="" type="checkbox"/> Other: Please describe: icomplaints EEO receives a daily HR Connect (HRC) download from The Department of Treasury system (Signed Memorandum of Understanding (MOU) & Interface Control Document (ICD) documentation is on file.). HRC is on a web server database. Name (First, MI, Last) User Identification (ID) (Employee ID from HR Connect) Date of Birth Pay Plan Grade Series Race Ethnicity Gender Employee Type Occupation Email Country	<input checked="" type="checkbox"/> Other: Please describe: icomplaints EEO receives a daily HR Connect (HRC) download from The Department of Treasury system (Signed Memorandum of Understanding (MOU) & Interface Control Document (ICD) documentation is on file.). HRC is on a web server database. _____

Bargaining Unit Union Code Union Code Translation Disability Description Org Code Home Address City/State/Zip Code Home Telephone Home Fax Personal Cell Phone Work Address City/State/Zip Code Work Telephone	
<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____

[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).

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

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).

Please check all boxes next to information that was provided to the individual.

- 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.

When the EEO Counseling Report is completed, the complainant is given a separate form containing the Privacy Act Statement. That statement contains all of the requirements above. Therefore, no privacy and/or civil liberties issues were identified.

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:

If yes, is there a statutory exception that would allow collection of the SSN (check all that apply):

- SSN disclosure is required by Federal statute or Executive Order. *If checked, please provide in the space provided below the legal citation to the applicable 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. *If checked, please provide the name of the system of records in the space provided below.;*

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.

The HRConnect Employee ID is used as an alternative to the SSN Therefore, no privacy and/or civil liberties issues were identified.

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(i)

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 refusal to provide a requested 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 iComplaints site in the counseling summary.

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 system tracks EEO cases (informal and formal) OCRD also uses the system to generate metrics for its annual report and provides statistical information derived from the system to EEOC (using EEOC Form 462). The EEOC uses the information that Treasury and other agencies provide in its annual statistical report on discrimination complaints. This usage is consistent with the Treasury's mission because it allows the bureau to track and manage Treasury's EEO process and generate its Form 462 annual report as well as the Notification and Federal Employee Antidiscrimination and Retaliation Act (NoFEAR Act) annual report.

iComplaints includes a number of critical features in order to track and manage EEO complaints and case processing. With its attention to tracking every potential nuance and variable in the EEO case management lifecycle, iComplaints provides complete assurance that every step in the EEO process is followed and accurate annual reports are generated. The Treasury iComplaints system services OCRD's Complaint Operations Division as well as the Department's 12 bureau EEO Offices.

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).

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

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)?

If yes or no, proceed to Section 5.1(b).

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 only documents contained in iComplaints system are the report of counseling, the acceptance letter (wherein the agency states the claims asserted that must be investigated), and any final agency decision (FAD) issued. These same documents are uploaded into the separate eComplaints system along with other documents related to the investigation of the formal complaint. The actual information contained in the iComplaints system is not used to make any determinations about individuals. This same information is, however, uploaded to the eComplaints system and may be used in that system to make adverse determinations. The eComplaints system is covered by a separate PCLIA that covers the uses of the information in that system.

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.

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

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 section (e)(5) of the [Privacy Act](#)?

No information in the iComplaints system is used to make determinations about any individual while it is in iComplaints. Therefore, fairness to the individual resulting from the use of the information while it is in the iComplaints system is not an issue. The same information is, however, uploaded to and maintained in the separate eComplaints systems and may be used to make adverse determinations about an individual. The manner in which accuracy, relevance, timeliness, and completeness are maintained are discussed in the PCLIA for the eComplaints system.

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?

The information maintained in the system (or used by the project) is not used as part of a matching program. Therefore, no privacy and civil liberties risks were identified in response to this section.

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?

The information contained in the EEO Counseling Report in the iComplaints system is obtained directly from the individual alleging a claim of discrimination. No information in the iComplaints system is used to make determinations about any individual while it is in iComplaints. Therefore, fairness to the individual resulting from the use of the information while it is in the iComplaints system is not an issue. The same information is, however, uploaded to and maintained in the separate eComplaints systems and may be used to make adverse determinations about an individual. The manner in which accuracy, relevance, timeliness, and completeness are maintained are discussed in the PCLIA for the eComplaints system. The FADs, which are also contained in iComplaints, typically include the Administrative Judge’s determinations regarding these data quality issues. For example, the Administrative Judge may determine in the FAD whether facts presented by the complainant or the agency lacked credibility or were irrelevant to the outcome of the case. Therefore, the nature of the process itself (including appellate relief) addresses accuracy, relevance, timeliness, and completeness issues by giving parties an opportunity to correct statements made by the opposing party or their witnesses.

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 from Treasury's HRConnect system (the Treasury system that houses departmentwide human resources information) is used to autopopulate forms with information from the complainant's human resources file. The information in HRConnect is provided by the employee when they apply for a position at Treasury and/or at the time they are hired. Therefore, the data has a greater likelihood of being accurate. Complainant's are also required to review the EEO Report of Counseling when it is completed to ensure the information is correct. Therefore, corrections can be done at that time or at any time during employment when data quality issues arise.

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](#))?

No information in the iComplaints system is used to make determinations about any individual while it is in iComplaints. Therefore, fairness to the individual resulting from the use of the information while it is in the iComplaints system is not an issue. The same information is, however, uploaded to and maintained in the separate eComplaints systems and may be used to make adverse determinations about an individual. The manner in which accuracy, relevance, timeliness, and completeness are maintained are discussed in the PCLIA for the eComplaints system.

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?

The information maintained in the EEO Report of Counseling is typically derived directly from the individual who is contemplating filing an EEO claim. Any issues related to the accuracy, timeliness and completeness of the information may be challenged by any party during the EEO investigation and hearing processes after a formal complaint is uploaded in the separate eComplaints system. These issues are discussed in the PCLIA for that system. Also, if a FAD is issued, it may address the accuracy, timeliness and completeness of the information provided by the individual. The FAD is also contained in iComplaints.

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? *If no, please analyze the privacy and/or civil liberties risks presented and mitigation efforts below.*

If corrections are required to any of the documents maintained in iComplaints, the revised document can be uploaded and the incorrect one removed or both versions can remain in the iComplaints site..

Section 5.3: Information sharing within the Department of the Treasury

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

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 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”)?

The information in the system is not technically shared with other bureaus within Treasury. The bureau EEO representatives that use iComplaints are technically representatives of the OCRD to the extent that they input information into the system regarding their EEO cases. Only OCRD may access all information in the system. Each bureau may only access information related to its own EEO cases. Therefore, there is no internal sharing. Each bureau sees only its own cases.

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?

The information in the system is subject to an MOU between Treasury and the US Postal Service (USPS) which maintains a multi-agency contract for EEO investigatory services. OCRD also has an

MOU/Interconnection Agreement with Treasury's HRConnect system which allows OCRD to pre-populate reports with employees' personal information, including employee ID, name, gender, pay, plan and level, race, series, employee type, date of birth, occupation, email address, country, first and second mailing address and phone numbers. There is not, however, any agreement that places restrictions on OCRD's use, maintenance, handling, or disclosure of the [PII](#) (though OCRD imposes its own restrictions).

Internal Information Sharing

Please complete the chart below for each internal Treasury bureau or office with which PII from the system or project is shared (add additional columns as needed). Discuss privacy risks and mitigation in the space provided below the chart.

There is no internal sharing because the bureaus are only able to see their own EEO case information that they input into the system.

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

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

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?

No privacy and civil liberties risks were identified because PII maintained in the system is not shared with agencies, organizations, or individuals external to Treasury. OCRD does not disclose PII outside Treasury. The only information shared outside Treasury is aggregate or statistical information from the data contained in iComplaints, which is used in OCRD's annual report and is provided to EEOC as required by law.

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? See 5 U.S.C § 552a(c).

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?

No privacy and civil liberties risks were identified because OCRD does not disclose Privacy Act information or PII from the system externally. Therefore, no accounting is required.

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)?

29 CFR §1614.601 and §1614.602 govern the EEO group statistics that federal agencies must collect and report to EEOC. The EEOC also 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?

No privacy and civil liberties issues were identified because iComplaints does not collect information from external agencies, organizations or individuals.

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](#)?

No privacy and civil liberties issues were identified.

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?

None of the Privacy Act protected information or other PII in iComplaints (as opposed to statistics generated based on PII in the system) is shared externally. Therefore, none of the information in the system is subject to an MOU 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. Therefore, no privacy and civil liberties issues were identified.

External Information Sharing Chart

[Section 5.4\(k\)](#) Yes No Is information from the system or project shared externally?

Privacy Act information and PII from the system are not shared externally. Therefore, no privacy and civil liberties issues were identified. The only information shared outside Treasury is aggregate or statistical information from the data contained in iComplaints in order to provide required reports to EEOC.

Obtaining Consent Prior to New Disclosures Not Included in the SORN or Authorized by the Privacy Act

<p>Section 5.4(i) <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> 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))?</p> <p><i>Information from the system is not shared externally. Therefore, no privacy and civil liberties issues were identified.</i></p>
--

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*.

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

System of Records
<p>Section 6.1(a) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Does the system or project retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? (see items selected in Section 4.2 above)</p>
<p>Section 6.1(b) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Was a SORN published in the <i>Federal Register</i> for this system of records?</p>
<p>Treasury/IRS 00.001 - Correspondence Files (including Stakeholder Relationship files and Correspondence Control Files)</p> <p>Treasury/IRS 34.037 - IRS Audit Trail and Security Records System</p> <p>Treasury/IRS 00.007 Employee Complaints and Allegation Referral Records</p>

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).

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each Section. All narrative responses should be included in the space provided at the end of each section.

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?

OCRDR is in the process of developing a single departmentwide counseling form to replace the preexisting individual forms used by each bureau. Once OCRDR obtains concurrence on a single, internal form for all of Treasury, OCRDR 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.

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

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?
Authorization to operate this system was obtained in June, 2015 (and is currently under review for renewal).

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 the System Administrator can add users, assign permissions and roles, review user accounts, update reference tables, view records, execute SQL queries, and view audit data. All other users have specific permissions assigned within the site to view specific information for their bureau.

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 MOU between HR Connect and Treasury sets the security levels that must be maintained by both parties when sharing employee data internally.in the MOU between Treasury and HRConnect.

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?
The MOU between HR Connect and Treasury sets the security levels that must be maintained by both parties when sharing employee data internally.in the MOU between Treasury and HRConnect.

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?
Reports regarding internal usage of the system by OCRD staff and contractors can be generated for internal oversight purposes. IComplaints does not monitor groups of people or individuals except system users (and that monitoring is limited to their use of the iComplaints system).

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.

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

Applicability of and Compliance With the Rehabilitation Act

Section 6.5(a) Yes No Will the project or system involve the development, procurement, maintenance

<p>or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)?</p> <p>Section 6.5(b) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> 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?</p> <p><i>No privacy and civil liberties issues were identified because iComplaints is in compliance with Section 508.</i></p>

Section 7: Redress

Please check the appropriate responses below and provide narrative responses as directed in the italicized guidance provided after each section. All narrative responses should be included in the space provided at the end of each section.

Access Under the Freedom of Information Act and Privacy Act
<p>Section 7.0(a) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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?</p> <p><i>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.</i></p>

Privacy Act Access Exemption
<p>Section 7.0(b) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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?</p> <p><i>Certain records in this system are exempt from 5 U.S.C. 552a(e)(4)(G) (allowing individuals to inquire whether there is information about them in a system of records), (e)(4)(H), and (e)(4)(I), and (f) (granting individuals access to records pertaining to them) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). See 31 CFR 1.36.</i></p> <p><i>Aggrieved persons who seek counseling services may elect to be anonymous during the informal counseling process (if the process ends there without the filing of a formal complaint). 29 CFR 1614.105(g) (“The Counselor shall not reveal the identity of an aggrieved person who consulted the Counselor, except when authorized to do so by the aggrieved person, or until the agency has received a discrimination complaint under this part from that person involving that same matter.”). Therefore, it would defeat the purpose of this provision in the regulation if the supervisor or other individual who is the subject of the informal complaint process (or others) could simply file a Privacy Act request to obtain this information. To allow the additional right to access and amend or correct the records submitted would undermine the investigatory process and destroy the integrity of the administrative record. If the aggrieved person chooses to go beyond the counseling phase and file a formal EEO complaint, the complainant must necessarily waive this right to anonymity.</i></p>

Additional Redress Mechanisms
<p>Section 7.0(c) <input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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)?</p> <p><i>No adverse determinations are made based on the information while it is contained in iComplaints. Therefore, no privacy or civil liberties issues were identified. Additional redress issues are addressed in the eComplaints PCLIA.</i></p>

Responsible Official

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

Approval Signature

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