Privacy and Civil Liberties Impact Assessment for the Office of Financial Research ("OFR") SharePoint and Collaboration Sites ("SharePoint")

September 6, 2016

Reviewing Official
Ryan Law
Acting Deputy Assistant Secretary
for Privacy, Transparency, and Records
Department of the Treasury

Bureau/Office Certifying Official
Wesley Fravel
Senior Information Security Specialist - Privacy
Office of Financial Research
Privacy and Civil Liberties Officer

Section 1.0: Introduction

It is the policy of the Department of the Treasury (hereinafter "Treasury" or "Department") and its Bureaus to conduct a Privacy and Civil Liberties Impact Assessment (hereinafter "PCLIA") when Personally Identifiable Information (hereinafter "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 (hereinafter "E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget (hereinafter "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 (hereinafter "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 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.

Section 2.0: Definitions

Agency – means any entity that falls within the definition of the term "executive agency", as defined in section 102 of title 31, United States Code, or "agency", as defined in section 3502 of title 44, United States Code.

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 – include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

Data mining – The term "data mining" means a program involving pattern-based queries, searches, or other analyses of 1 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) or the Privacy Act, 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 – the use of digital technologies to transform government operations in order to improve effectiveness, efficiency, and service delivery.

Federal information system – 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 Notice of proposed rulemaking (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 make any revisions to 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 – 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) – 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, Section 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 rulemaking (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) – "means, 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. The definition of this term also incorporates by reference the definition of PII in OMB Memorandum 06-19[1] and the definition of term

[1] "Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric

"Information in Identifiable Form" as defined in § 208(d)[2] of the E-Government Act of 2002, Pub. L.107-347, 116 Stat. 2899 and as further defined in OMB M 03-22.[3]

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.

Reviewing Official – The Deputy Assistant Secretary, Privacy, Transparency and Records who reviews and approves all PCLIAs as part of their 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 the Department of the Treasury (i.e., external sharing), the use of such record for a purpose which is compatible with the purpose for which it was collected.

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

---

records, etc., including any other personal information which is linked or linkable to an individual.

2 "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

3 "Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)"

agency records under the Freedom of Information Act (5 U.S.C. 552) 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 the Freedom of Information Act (5 U.S.C. 552) 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 (as defined in the Privacy Act) 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.

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 his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and (I) the categories of sources of records in the system.

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

Section 3.0: System Overview

Microsoft SharePoint ("SharePoint") is an application providing an information-sharing platform, document management platform, and workflow platform that allows users within an organization to collaborate, share, and manage electronic information within workgroups and project teams.

Through SharePoint, organizations can build unique sites where users can easily share files, engage in simultaneous editing of documents, and create document libraries and knowledge bases. SharePoint uses central management, governance, and security controls to facilitate monitoring and maintenance of content within the total environment and within specific SharePoint sites.

OFR is conducting this PCLIA to evaluate the general privacy risks involved in deploying SharePoint.

Section 3.1: System/Project Description

Currently, OFR leverages Microsoft SharePoint 2013 as deployed enterprise-wide across Treasury. The system runs on Treasury's internal servers, and Treasury SharePoint sites are not accessible to anyone outside of the Treasury. OFR staff use SharePoint to effectively and efficiently perform the OFR's research and other activities.

As part of a larger effort to migrate information technology capabilities from those purchased and managed by Treasury to those developed and supported by OFR, OFR will procure and host its own version of SharePoint. For its version of SharePoint, OFR will host Microsoft SharePoint 2013 on secure, internal OFR servers, with access limited to OFR employees, contractors, limited Departmental Offices (DO) and Financial Stability Oversight Council (FSOC) employees, and other OFR personnel (for the purposes of this PCLIA, "other personnel" includes detailees, "IPAs" under the Intergovernmental Personnel Act, interns, and clerks).

SharePoint, as used by the OFR, will provide a selection of functionalities to improve business collaboration and communications, including browser-based process management modules, enterprise search modules, workflows, personalization, blogs and wikis, and advanced indexing and searching capabilities. OFR mainly uses SharePoint to host Division/Office websites, shared workspaces, information repository and document storage. Authorized users can manipulate certain controls or interact with pieces of content, such as lists and document libraries. SharePoint's security and governance model allows site owners to manage content and security for sites under their responsibility. Acting in coordination with Division/Office SharePoint points of contact, site owners/administrators are responsible for monitoring and maintaining the content of their respective sites. The site owners/administrators ensure that information collected or placed into the OFR SharePoint sites are appropriate and in line with OFR data classification, security, and retention policies. In addition, OFR uses additional supporting software to implement a robust security model of monitoring and auditing access to content, administrative actions, and overall governance of the OFR SharePoint environment.

OFR SharePoint sites serve as a secure workspace for collaboration on active documents and other content for business purposes. As such, the OFR's SharePoint instance will maintain various, but limited types of personally identifiable information (PII) as necessary to accomplish authorized OFR business needs.

As an example, types of PII that may be included in documents, files, or workflows maintained in or processed by SharePoint include names and contact information (personal and business) of current and prospective OFR employees, contractors, and other personnel (in the form of organization charts, contact lists, etc.); educational and employment related history (in the form of CVs, resumes, bios, etc.); pictures, video and audio-recordings from OFR publications or events (both internal and external); and similar information used for administrative processes such as User Access Requests for data, ticketing services for the OFR Help Desk, and requests for training, external event attendance, etc. In general, all electronically stored information found on OFR SharePoint sites, including PII, must be related to an official OFR business need.

By policy, users of OFR's SharePoint environment are prohibited from publishing or storing sensitive or confidential files and information in areas of the portal not intended specifically for that purpose. Individual site owners are responsible for identifying and classifying all files and information published in their site in accordance with OFR's data classification procedures. Further, users are strongly discouraged from using SharePoint to store files or documents containing sensitive PII (e.g. SSNs, account numbers, etc.). Individual sites are required to be reviewed on a regular basis by site owners to ensure only appropriate content is published and that access and security controls around such content is appropriate and in alignment with existing OFR policies and procedures.

SharePoint also provides a secure work area, known as "My Site," where users have the capability to post a professional picture and enter business-related and personal information, such as their professional biographies and skills and interests, for others within OFR to view. The public profile information is managed by the individual users, and the users may choose privacy levels that help ensure that data stored in their profiles is visible only to intended parties within OFR.

Number of Individuals Maintained in the System or Project		
☒ 0 – 999	☐ 1000 – 9,999	☐ 10,000 – 99,999
☐ 100,000 – 499,999	☐ 500,000 – 999,999	☐ 1,00,000+

Section 3.2: Purpose Specification

Data maintained in or processed in OFR SharePoint sites is relevant and necessary to accomplish authorized OFR business needs. The specific types of PII maintained within SharePoint vary based on the business need(s) for which each SharePoint site was designed (i.e., research, external affairs and communications, legal, vendor/contract management, Human Resources/personnel, etc.). In general, data, including PII, is used for administrative purposes. Section(s) 4 and 5 of this PCLIA discuss the individual data elements and their use in the system.

Section 3.3: Authority to Collect

The statutory authorities for operating this system or performing this project are:

Statute	Description
Dodd-Frank Wall Street Reform Act and Consumer Protection Act (Pub.L. 111–203, H.R. 4173), Section 153.	Establishes the OFR and authorizes the OFR Director to manage administrative functions of the office.
44 U.S.C. § 3101	Instructs the head of each federal agency to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."

Section 4.0: 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." See 5 U.S.C. § 552a(e)(1).

The Privacy Act allows federal agencies to exempt records from the relevant and necessary requirement if certain conditions are met. This includes issuing a Notice of Proposed Rulemaking (hereinafter "NPRM") to solicit public opinions on the proposed exemption and issuing a Final rule after addressing any concerns raised by the public in response to the NPRM. 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 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?

Explanation for Answers in Sections 4.1(a) thru 4.1(d): OFR SharePoint sites do not currently operate as a Privacy Act System of Records (SORs), however, they may be used to process and store information that is subject to the Privacy Act.

Information subject to the provisions of the Privacy Act stored within or processed by OFR SharePoint sites is generally limited to that which is covered by:

***Treasury .014 – Department of the Treasury SharePoint User Profile Services*:** Includes employee, contractor, and other personnel information included in the tool (i.e. contact information, limited biographical information used in org charts, contact lists, etc.)

***Treasury .015 – General Information Technology Access Account Records*:** Includes information from OFR employees, contractors, and other personnel that is used to populate OFR's access management system and grant authorized users access to the SharePoint application, or to conduct other similar routine administrative functions).

***Treasury .001 – Treasury Personnel and Payroll System*:** Includes employment information, resumes, CVs, and similar information of current and prospective OFR employees, contractors, and other personnel.

***Treasury .017 – Correspondence and Contact Information*:** Includes information related to engaging members of the public who partner with the OFR in support of its research mission.

In general, most of the data, including PII, maintained or processed in OFR SharePoint sites is not collected by the OFR directly. Data is derived from primary sources or source systems and then leveraged within SharePoint sites as necessary for a specific business purpose or need. For each primary data source subject to the Privacy Act, PII was collected by the Treasury Department directly, in accordance with Treasury-wide rules, procedures, and processes, including an assessment to

determine which PII types are relevant and necessary for the original (and any identified secondary) business purposes.

While OFR does not oversee these assessments, it does limit its request and use of such information within OFR SharePoint sites to that which is relevant and necessary for clearly articulated OFR business processes. For example, for data collected to grant OFR employees, contractors, and authorized users access to applications and databases hosted on or supported by the OFR's Analytical Environment (OFRAE), such information is governed in accordance with the Treasury System of Records Notice (SORN), Treasury .015 – General Information Technology Access Account Records (GITAARS). This information is limited to that which is necessary to grant access to and use of OFR information technology resources, including OFR SharePoint sites. Such information is not maintained within the SharePoint sites, but may be processed by it in order to grant access and associated permissions.

As another example, for information used to populate individual "My Site" public profiles and organizational charts within OFR SharePoint sites, OFR pulls the following types of business and organizational tree information from OFR's access management system to populate individual users' profile pages: employee name, work email address, work telephone number, title, division, supervisors, work groups, etc. Employees may also choose to further populate their individual "My Site" profiles with a photograph, a description of their skills/experience, or educational background, etc. This information is governed by the Treasury SORN, Treasury .014 – Department of the Treasury SharePoint User Profile Services.

OFR regularly reviews its user access processes as well as its collection and use(s) of PII to ensure the appropriate information is captured to for the identified business need. Further, by policy, users of OFR's SharePoint environment are prohibited from publishing/storing sensitive or confidential files and information in areas of the portal not intended specifically for that purpose. Individual site owners are responsible for identifying and classifying all files and information published in their site in accordance with OFR's data classification procedures. By policy, individual sites are required to be reviewed on a regular basis by site owners to ensure only appropriate content is published and that access and security controls around such content is appropriate and in alignment with existing OFR policies and procedures.

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.

To promote transparency, OFR has indicated by asterisk (*), those fields for which OFR maintains or processes information on members of the public through the OFRAE.

Biographical/General Information Regarding Individuals		
☒ Name	☐ Gender	☒ Group/Organization Membership
☐ Birth Date	☐ Race/Ethnicity	☒ Military Service Information *Limited to an individual's indication of military service on their "My Site" profiles page within the OFR*

		SharePoint environment or where such information is shared in the resume of a prospective OFR employee.
☒ Home Physical Mailing Address	☐ Citizenship	☐ Marital Status
☒ Personal Cell Number	☐ Nationality	☐ Mother's Maiden Name
☒ Personal Home Phone or Fax Number	☐ Country of Birth	☒ Spouse Information* **Generally limited to that which may be included in Emergency Contact information referenced below.*
☒ Personal e-mail address	☐ City or County of Birth	☒ Children Information* **Limited to OFR employees who participate in annual "Bring Your Child to Work Day"*
☐ Alias (including nickname)	☐ Immigration Status	☐ Information about other relatives.
☒ Education Information* **To include resumes and CVs of board members and researchers conducting research on behalf of OFR, as well as OFR employees, contractors, and applicants for OFR positions. May also include limited educational information included by OFR employees on their "My Site" profile within the OFR SharePoint environment.*	☐ Religion/Religious Preference	☐ References or other information about an individual's friends, associates or acquaintances.
☐ Personal Financial Information (including loan information)	☐ Passport Information	☐ 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.)	☒ Contact lists and directories	☒ Other (please describe): Emergency contact information of OFR employees, contractors, and other personnel including names, personal phone numbers and email addresses. See below.
☐ Network communications data	☐ Device settings or preferences (e.g., security level, sharing options, ringtones).	☐ Other (please describe):
☐ Other (please describe):	☐ Other (please describe):	

Identifying Numbers Assigned to Individuals	
☒ Full Social Security number* **Limited to those potentially included/collected via resumes submitted for positions at the OFR and being reviewed/considered. Guidance and policy strongly discourages users from using the SharePoint environment for storing and reviewing these types of documents. Further, OFR does not actively collect or seek this information.*	☐ Personal Bank Account Number
☒ Truncated Social Security Number (e.g., last 4 digits) **See above.*	☐ Health Plan Beneficiary Number
☐ Employee Identification Number	☐ Credit Card Number
☐ Taxpayer Identification Number	☐ Patient ID Number
☐ File/Case ID Number	☐ Vehicle Identification Number
☐ Alien Registration Number	☐ Driver's License Number
☐ Personal device identifiers or serial numbers	☐ License Plate Number
☐ Internet Protocol (IP) Address (where known to belong to an individual or unknown whether the IP address belongs to an individual or organization)	☐ Professional License Number
☐ Other (please describe):_____	

Medical/Emergency Information Regarding Individuals		
☐ Medical/Health Information	☐ Worker's Compensation Act Information	☐ Patient ID Number
☐ Mental Health Information	☐ Disability Information	☒ Emergency Contact Information (e.g., a third party to contact in case of emergency)
☐ Other (please describe): _____		

Biometrics/Distinguishing Features/Characteristics of Individuals		
☐ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.)	☒ Signatures* **To include OFR employees, contractors, and other personnel on administrative documents such as training requests, letters, or certificates.*	☐ Vascular scans
☐ Fingerprints	☒ Photos* **To include OFR employees, contractors, and individuals who attend OFR-sponsored events, or individual photos included by OFR staff as part of their "My Site" profile page, or as part of OFR*	☐ Retina/Iris Scans

	organizational charts (submission is voluntary).	
☐ Palm prints	☒ Video* **To include recordings of presentations or speeches made by OFR employees or officials, or events in which OFR employees or officials are participants (e.g. congressional hearings, conference presentations, news interviews, internal presentations, etc.)*	☐ Dental Profile
☒ Voice audio recording **To include recordings of presentations or speeches made by OFR employees or officials, or events in which OFR employees or officials are participants (e.g. congressional hearings, conference presentations, news interviews, internal presentations, etc.)*	☐ Scars, marks, tattoos	☐ DNA Sample or Profile
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe):

Specific Information/File Types That Include Information Regarding Individuals		
☐ Taxpayer Information/Tax Return Information	☐ Law Enforcement Information	☐ Security Clearance Information
☐ Civil/Criminal History Information/Police Records	☐ National Security/Classified Information	☐ Bank Secrecy Act Information
☐ Protected Information (as defined in Treasury Directive 25-10)	☐ Case files	☒ Personnel Files *To include limited information (notes of conversations, etc.) on OFR employees or prospective employees NOT captured in the official systems used for this purpose, or charts of employees, etc. used for workforce planning and budgeting.*
☐ Information provided under a confidentiality agreement	☐ Information subject to the terms of an international or other agreement	☐ Other (please describe): _____

Audit Log and Security Monitoring Information		
☒ User ID assigned to a user of Treasury IT* **See "Other" below.*	☐ Date and time an individual accesses a facility, system, or other IT	☐ Files accessed by a user of Treasury IT
☐ Passwords generated by 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

☐ Video of individuals derived from security cameras	☐ Biometric information used to access Treasury facilities or IT	☐ Public Key Information.
☐ 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.	☐ Other (please describe): _____

Other	
☒ Other (please describe): Employee names and related administrative info (including user IDs, etc.) connected to User Access Requests for data, ticketing services for the OFR Help Desk, and requests for training, external event attendance, etc.	☐ Other (please describe): _____
☐ Other (please describe): _____	☐ Other (please describe): _____

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

Generally, data maintained in OFR SharePoint sites is obtained and uploaded by OFR employees, contractors, and other authorized users in connection with their various job responsibilities. The sources of such data vary based on the nature of the data. With regards to PII processed or maintained within OFR SharePoint sites, a majority of such data is retrieved (automatically) from existing source systems, and is not collected directly from impacted individuals, for example, information used to grant permissions within OFR SharePoint sites, or to populate user and OFR employee directories. Other information is manually retrieved from other source systems. For example, contact information for individuals who have corresponded with or are receiving correspondence from the OFR, in the form of a letter being drafted and edited within an OFR SharePoint site. In many cases, this data is subject to the Privacy Act. Section 4 of this PCLIA discusses the implicated Privacy Act source systems and the data derived from each.

Some information is collected directly from individuals. For example, information is provided by OFR employees and SharePoint users to populate their individual "My Site" public profile pages. Providing such information is voluntary and may include things like professional photographs, skills and interests, educational information, and other similar business-related professional personal information users share about themselves. Users are limited to including information outlined in the provided fields on their individual "My Site" public profile page. Users retain the right to modify or edit the information at any time. Further, users are provided a privacy notice on the main OFR SharePoint directory page regarding the collection and use of this information.

Additionally, some information, such as emergency contact lists of employees, audio and video recordings of OFR employees or officials giving speeches or presentations in their professional capacity, and notes made on administrative processes, such as scheduling interviewees, or workforce planning, etc. is included within the OFR SharePoint sites. Finally, some resumes of prospective employees or individuals who wish to or have engaged with OFR on its research mission may also be included.

The chart below outlines the three "types" of data sources for data included in OFR SharePoint sites and the PII identified in Section 4.2 that was acquired from each source.

OFR Employees/Contractors/ Other Personnel	Individuals Who Engage with OFR on Research Mission	Treasury HRConnect/OFR Access Management System
Specific PII identified in Section 4.2 that was acquired from this source: – Employee, contractor, or other personnel name – Emergency contact information, including limited personal contact information – Personnel and administrative notes, including workforce planning, etc. – Signatures – Photos – Video and audio recordings	**Specific PII identified in Section 4.2 that was acquired from this source:** – Names; – Business or professional contact information as part of mailing lists, or credits in research papers and products, or included in draft and finalized correspondence, etc. – Resumes and CVs of board members and researchers conducting research on behalf of OFR, or current or prospective OFR employees contractors, or other personnel; – Other identifying information included on resumes or CVs (see 4.2 regarding the collection of Social Security numbers).	**Specific PII identified in Section 4.2 that was acquired from this source:** – Employee, contractor, or other personnel name – Business email address – Business phone number – Business address – Title – Supervisor/team/group name for organizational chart/employee directory
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):**	**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 Please identify the form name (or description) and/or number (e.g., OMB Control Number): N/A	☐ 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): _____	☐ 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): _____
☒ Received in paper format other than a form.	☒ 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.	☐ 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	☐ Accessed and downloaded or otherwise acquired via the internet
☒ Email	☒ Email	☐ Email
☒ Scanned documents uploaded to the system.	☒ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.
☐ Bulk transfer	☐ 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).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
☐ Fax	☒ 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	☐ Extracted from notes of a phone interview or face to face contact
☐ Other: Please describe:	☐ Other: Please describe: _____	☒ Other: Please describe: Data is acquired by OFR's PDS to populate the OFR's access management system, which in turn is used to populate basic user information in SharePoint sites and manage permissions, access, etc.
☐ Other: Please describe: _____	☐ Other: Please describe: _____	☐ 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 him, if any, of not providing all or any part of the requested information." See 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) ☐ N/A 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 or 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.

Explanation for Answers in Sections 4.4(a) thru 4.4(c): A large portion of information processed in SharePoint is not collected directly from individuals and is retrieved from other sources, as discussed in Section 4.3.

Information collected directly from the individual for inclusion in an OFR SharePoint site, is generally limited to professional biographical information input by employees and users to their "My Site" user profile page. Users are provided a privacy notice on the directory page for the OFR SharePoint site.

Other PII processed by or within OFR SharePoint sites that is subject to the Privacy Act is not collected directly by the OFR, and is managed in accordance with requirements outlined in Section e(3) of the Privacy Act by the respective agencies responsible for the original collection and maintenance of such information.

Use of Social Security Numbers

Social Security numbers (hereinafter "SSN") are commonly used by identity thieves to commit fraudulent acts against individuals. Therefore, as a matter of policy, federal agencies are required to eliminate the use of SSNs (subject to certain exceptions).

In addition, the Privacy Act, as amended, 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 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. See Pub. L. 93–579, § 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 Were steps taken to explore alternatives to the use of SSNs as a personal identifier in the system or project and were any resulting actions taken to eliminate unnecessary uses?

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?

☐ SSN disclosure is required by Federal statute;

☐ 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; or

☐ when the information is collected, individuals are given notice whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Explanation for Answers in Sections 4.4(d) thru 4.4(f): Some OFR SharePoint sites may include documents that include SSNs, full or truncated. This generally occurs via resumes submitted for positions at the OFR which are being reviewed or considered. Guidance and policy strongly discourages users from using the SharePoint environment for storing and reviewing these types of documents.

By policy, users of OFR's SharePoint environment are prohibited from publishing or storing sensitive or confidential files and information in areas of the portal not intended specifically for that purpose. Individual site owners are responsible for identifying and classifying all files and information published in their site in accordance with OFR's data classification procedures. Further, individual sites are required to be reviewed on a regular basis by site owners to ensure only appropriate content is published and that access and security controls around such content is appropriate and in alignment with existing OFR policies and procedures.

OFR does not actively collect or seek this information.

First Amendment Activities

The Privacy Act requires 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." See 5 U.S.C. § 552a.(e)(7).

Section 4.4(g) ☐ Yes ☒ No Does the system or project maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? ☐ 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.
Explanation for the Answer to Section 4.4(g): OFR SharePoint sites do not maintain any information describing how any individual exercises their rights guaranteed by the First Amendment.

Section 5.0: Maintenance, use and sharing of the information

The following sections require a clear description of the system's or project's use(s) 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 specific types of PII maintained or processed within OFR SharePoint sites vary based on the business need(s) for which each SharePoint site was designed (i.e., research, external affairs and communications, legal, vendor/contract management, Human Resources/personnel, etc.). Data maintained in or processed, including PII, is limited to only that which is necessary for a specific business purpose. Generally, data is used to facilitate daily business functions of the OFR, like managing employee workloads, facilitating internal communication among employees, allowing employees to collaborate on work products such as research papers, correspondence, public and internal presentations, and other similar, related tasks. Sections 4.2 and 4.3 of this PCLIA address the individual data elements processed in OFR SharePoint sites, their use(s), and the nature of their collection.

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." See 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, etc.)? **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?
Explanation of the Answer to Section(s) 5.1(a) through 5.1(c): Information processed or maintained in OFR SharePoint sites is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

Data Mining

As required by Section 804 of the Implementing the 9/11 Commission Recommendations Act of 2007 (hereinafter "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?
Explanation of the Answer to Section 5.1(d): OFR will not use information processed or maintained in OFR SharePoint sites to conduct "data-mining" activities as that term is defined in 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." See 5 U.S.C § 552a.(e)(5). If a particular system of records meets certain requirements (including the NPRM process discussed 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?

Explanation of the Answer to Section 5.2(a): Information processed or maintained in OFR SharePoint sites that is subject to the Privacy Act is not exempt from the timeliness and completeness requirements of section (e)(5) of the Privacy Act.

Computer Matching

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act for the purpose of 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? See 5 U.S.C § 552a.(o)(J). **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?
Explanation of Answers to Sections 5.2(b) through 5.2(e): Information processed by or maintained in OFR SharePoint sites that is subject to the Privacy Act is not subject to or part of a matching program.

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." See 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 ☒ N/A 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?
Explanation of the Answer to Section 5.2(f): Information processed or maintained in OFR SharePoint sites is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

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 not all of the information being merged matches a particular individual (i.e., partial matches)?
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?
Explanation of Answers to Sections 5.2(g) through 5.2(k): PII processed by or maintained in OFR SharePoint sites is not merged with other electronic or non-electronic information from internal or external sources.

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 (regardless of whether 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)?

Explanation of the Answer to Sections 5.2(l) and 5.2(m): Information processed or maintained in OFR SharePoint sites is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs. Processes and procedures governing data, including PII are described below in Section 5.2(n).

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

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

Explanation of the Answer to Sections 5.2(n): As previously discussed, a large portion of the information, including PII, maintained or processed by the system is retrieved from source systems or otherwise not collected directly from the individual. As such, the OFR does not receive explicit assurances of the accuracy, relevance, timeliness, and completion of such information. However, for information obtained from source systems which implicate the Privacy Act, such information is collected in accordance with Treasury-wide rules, procedures, and processes, including considerations for data quality and accuracy.

In some cases, individuals provide their own information, either through the source system, or directly into the OFR SharePoint site. In such cases, the information is considered accurate, timely, and complete. Further, individuals may change, amend, or otherwise update the information as necessary. For example, information in the OFR's access management system to populate user profiles and grant permissions within SharePoint sites, provided by Treasury HRConnect is originally collected directly from an individual by Treasury Departmental Offices (DO). The employee and contractor contact information provided by Treasury DO is relied upon as accurate and complete as it is the system of record for employee and contractor data and is collected directly from the individual. Similarly, additional professional biographical information provided by OFR employees for their "My Site" public profile page is voluntarily provided directly by the employee and can be updated, amended, or deleted at any time.

As outlined above, no information processed by or maintained in OFR SharePoint sites is used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

Disseminating Notice of Corrections 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?

Explanation of the Answer to Sections 5.2(o) and 5.2(p): OFR SharePoint sites do not currently operate as a Privacy Act System of Records (SOR), however, they may be used to process and store information that is subject to the Privacy Act, including provisions requiring the dissemination for corrections or amendments of PII and notification of impacted individuals. As such PII which OFR receives from source systems is updated by the agency which provided the PII. That said, for PII collected directly from individuals in the system, individuals may access, amend, or correct such information, and would thus be notified (at the time of update) of the change to their information.

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 or offices? **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")?
Explanation of the Answer to Sections 5.3(a): Information maintained or processed by OFR SharePoint sites may include PII that is shared with other components of Treasury. However, the OFR SharePoint environment and individual sites are not the primary method for such sharing. OFR SharePoint sites are hosted on secure, internal OFR servers, with access limited to OFR employees, contractors, and limited DO and FSOC personnel. Sharing of this information would occur outside of the SharePoint mechanism on a need-to-know basis, and only in accordance with requirements outlined for the source system or dataset.

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?

Internal Information Sharing Chart

Internal Recipient's Name (e.g., bureau or office)	OFR
Purpose of the Sharing	Authorized users access or request access to PII maintained on the system relative to the business purpose for which the PII exists. For example, an OFR employee, by default, has access to other users' public profile "My Site" pages, as well as organizational charts and directories, which include the names, business contact information, etc. of OFR employees. In another scenario, an OFR employee may be granted access to a specific OFR SharePoint site, by the site's administrator, in

	order to access an OFR draft white paper, a piece of correspondence, or a resume of potential candidates for a detail assignment with OFR. In both of these scenarios, access is limited to those with a clearly defined business need-to-know, and in accordance with the policies and procedures established for the OFR SharePoint environment.
PII Shared	PII shared is limited to that which is necessary for a specific business purpose or request as described above in "Purpose of Sharing."
Applicable Statutory or Regulatory or Restrictions on Information Shared	OFR has a statutory obligation under the Dodd-Frank Act ("Act") to protect proprietary data from unauthorized disclosure. That said, by policy, users are prohibited from storing sensitive or confidential information in areas of the SharePoint environment, not deemed appropriate for such data. Further, OFR employees are strongly discouraged from storing such data, including confidential data, or data otherwise subject to similar restrictions (proprietary, etc.) within the SharePoint environment. Administrators for each SharePoint site are responsible (by policy) for regularly reviewing their sites to ensure only appropriate information is maintained or processed by the system.
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	Where applicable, data referenced above are subject to a form of written agreement including licenses, information sharing agreements and memoranda of understanding. Each agreement contains provisions related to the access, use and disclosure of the data and other information provided under the agreement. A copy of each contract is maintained on file by Treasury Bureau of Financial Services (BFS) and OFR. All other agreements are maintained on file by the OFR Chief Counsel. However, as discussed, OFR employees are strongly discouraged from storing such data, including confidential data, or data otherwise subject to similar restrictions (proprietary, etc.) within the SharePoint environment. Administrators for each SharePoint site are responsible (by policy) for regularly reviewing their sites to ensure only appropriate information is maintained or processed by the system.
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling or Sharing of PII Received	See above.
Method of PII Transfer (e.g., paper/ oral disclosures/ magnetic disk/portable device/email fax/other (please describe if other)	The method of PII transfer within the SharePoint environment and SharePoint sites is electronic only.

Explanation for Responses in the Internal Information Sharing Chart: Authorized users access or request access to PII maintained on the system relative to the business purpose for which the PII exists. For example, an OFR employee, by default, has access to other users' public profile "My Site" pages, as well as organizational charts and directories, which include the names, business contact information, etc. of OFR employees. In another scenario, an OFR, DO, or FSOC employee may be granted access to a specific OFR SharePoint site, by the site's administrator, in order to access an OFR draft white paper, a piece of correspondence, or a resume of potential candidates for a detail assignment with OFR. In both of these scenarios, access is limited to those with a clearly defined business need-to-know, and in accordance with the policies and procedures established for the OFR SharePoint environment. By policy, users are prohibited from storing sensitive or confidential information in areas of the SharePoint environment, not deemed appropriate for such data. Further, OFR employees are strongly discouraged from storing such data, including confidential data, or data otherwise subject to similar restrictions (proprietary, etc.) within the SharePoint environment. Administrators for each SharePoint site are responsible (by policy) for regularly reviewing their sites to ensure only appropriate information is maintained or processed by the system.

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?
Explanation of the Answer to Section 5.2(a): Information maintained in or processed by an OFR SharePoint site is not shared with agencies, organizations, or individuals external to Treasury except as required by law or as outlined in applicable SORNs or similar notices and agreements that pertain to the source system and information processed by the system.

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 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 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?

Explanation of Answers to Sections 5.4(b) through 5.4(f): OFR SharePoint sites do not currently operate as a Privacy Act System of Records (SORs), however, they may be used to process and store information that is subject to the Privacy Act.

Data is derived from primary sources or source systems and then leveraged within SharePoint sites as necessary for a specific business purpose or need. For each primary data source subject to the Privacy Act, PII was collected by the Treasury Department directly, in accordance with Treasury-wide rules, procedures, and processes, including a process by which disclosures are accounted for.

Further, it is important to note that PII processed by an OFR SharePoint site is only shared with external information sharing partners as required by law, or as outlined in the specific SORN, notice, or similar agreement which governs a particular information collection processed by or maintained on an OFR SharePoint site.

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 (e.g., 26 U.S.C § 6103 limits disclosure of tax returns and return information) on the sharing of any of the information or records maintained in the system or by the project?

Explanation of the Answer to Section 5.4(g): Federal statutes such as the Trade Secrets Act and the Dodd-Frank Act require OFR to maintain and preserve the confidentiality of proprietary information received from third parties. However, as stated above, OFR employees are strongly discouraged from storing such data, including confidential data, or data otherwise subject to similar restrictions (proprietary, etc.) within the SharePoint environment. Administrators for each SharePoint site are responsible (by policy) for regularly reviewing their sites to ensure only appropriate information is maintained or processed by the system.

Memorandum of Understanding Related to External Sharing

Section 5.4(h) ☒ Yes ☐ No ☐ N/A Does Treasury (including bureaus and offices) have an MOU, or 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?

Explanation of the Answer to Section 5.4(h): OFR SharePoint sites store and process various data. Data is derived from primary sources or source systems and then leveraged within SharePoint sites as necessary for a specific business purpose or need. Any such sharing would be governed by the terms of the applicable SORN, notice, contract, license, or other agreement governing use of the source system or source data which is maintained or processed within an OFR SharePoint site. However, please note that PII processed by OFR SharePoint sites is only shared with external information sharing partners as required by law, or as outlined in the specific SORN, notice, or agreement which governs the original information collection or source system. Further, the OFR SharePoint environment and individual sites are not the primary method for such sharing. OFR SharePoint sites are hosted on secure, internal OFR servers, with access limited to OFR employees and contractors. Sharing of this information would occur outside of the SharePoint mechanism on a need-to-know basis, and only in accordance with requirements outlined for the source system or dataset.

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

Section 5.4(i) ☒ 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, an international agreement or treaty or contract with private vendor) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII?

Explanation of the Answer to Section 5.4(i): In general, OFR SharePoint sites store and process various data. Data is derived from primary sources or source systems and then leveraged within SharePoint sites as necessary for a specific business purpose or need. Data is governed by various agreements, notices, etc. in accordance with the source data or source system. Section 5.3(c) includes more information on agreements governing PII processed by or maintained within OFR SharePoint sites. Further, as discussed in Section 5.4, Further, the OFR SharePoint environment and individual sites are not the primary method for such sharing. OFR SharePoint sites are hosted on secure, internal OFR servers, with access limited to OFR employees and contractors, and limited DO and FSOC personnel. Sharing of this information would occur outside of the SharePoint mechanism on a need-to-know basis, and only in accordance with requirements outlined for the source system or dataset.

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

Section 5.4(j) ☒ 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 in which Treasury limits or places conditions on an external party's use, maintenance, handling or disclosure of PII shared by Treasury?

Explanation of the Answer to Section 5.4(j): PII processed by or maintained in OFR SharePoint sites is only shared with external information sharing partners as required by law, or as outlined in the specific SORN, notice, or agreement which governs the original information collection or source system. Section 5.3(c) includes more information on agreements governing PII included in OFR SharePoint sites. By policy, users of OFR's SharePoint environment are prohibited from publishing/storing sensitive or confidential files and information in areas of the portal not intended specifically for that purpose. Individual site owners are responsible for identifying and classifying all files and information published in their site in accordance with OFR's data classification procedures. Further, users are strongly discouraged from using SharePoint to store files or documents containing sensitive PII (e.g. SSNs, account numbers, etc.). By policy, individual sites are required to be reviewed on a regular basis by site owners to ensure only appropriate content is published and that access and security controls around such content is appropriate and in alignment with existing OFR policies and procedures.

External Information Sharing Chart				
Section 5.4(k) ☒ N/A				
External Recipient's Name	N/A			
Purpose of the Sharing	N/A			
PII Shared	N/A			
Content of Applicable Routine Use/Citation to the SORN	N/A			
Applicable Statutory or Regulatory or Restrictions on Information Shared	N/A			
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Providing/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of PII)	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			
Method(s) Used to Transfer PII (e.g., paper/ oral disclosures/ magnetic disk/portable device/email fax/other (please describe if other)	N/A			

Obtaining Consent Prior to New Disclosures Not Included in the SORN
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))?
Explanation of the Answer to Section 5.4(l): OFR SharePoint sites do not currently operate as a Privacy Act System of Records (SORs), however, they may be used to process and store information that is subject to the Privacy Act. As such, PII which OFR receives from source systems is updated (and consent obtained) by the agency which provided the PII via the original data collection or source system. Further, PII processed by OFR SharePoint sites is only shared with external information sharing partners as required by law, or as outlined in the specific SORN, notice, or agreement which governs an information collection processed or maintained. The OFR SharePoint site is not the primary method of such sharing if it occurs.

Section 6.0: Legal 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 all 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 ☐ N/A 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) **Section 6.1(b)** ☒ Yes ☐ No ☐ N/A Was a SORN published in the *Federal Register* for this system of records?
Explanation of the Answers to Sections 6.1(a) and 6.1(b): OFR SharePoint sites do not currently operate as a Privacy Act System of Records (SORs), however, they may be used to process and store information that is subject to the Privacy Act. Information subject to the provisions of the Privacy Act stored within or processed by OFR SharePoint sites is generally limited to that which is covered by: ***Treasury .014 – Department of the Treasury SharePoint User Profile Services*:** Includes employee and contractor information included in the tool (i.e. contact information, limited biographical information used in org charts, contact lists, etc.). ***Treasury .015 – General Information Technology Access Account Records*:** Includes information from OFR employees, contractors, and other personnel that is used to populate OFR's access management system and grant authorized users access to the SharePoint application, or to conduct other similar routine administrative functions).

***Treasury .001 – Treasury Personnel and Payroll System*:** Includes employment information, resumes, CVs, and similar information of current and prospective OFR employees, contractors, and other personnel.

***Treasury .017 – Correspondence and Contact Information*:** Includes information related to engaging members of the public who partner with the OFR in support of its research mission.

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 personally identifiable information 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 (hereinafter "ICR") and receive OMB approval?
Explanation of the Answers to Sections 6.2(a) through 6.2(c): To date, OFR has not initiated a data collection subject to the requirements of the Paperwork Reduction Act.

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 Has the Archivist of the United States approved a retention schedule for the records maintained in the system or by the project? **Section 6.3(b)** ☒ Yes ☐ No Do General Records Schedules (hereinafter "GRS") apply to the records maintained in the system or by the project? **Section 6.3(c)** ☐ Yes ☐ No ☒ N/A If the Archivist of the United States has not approved a retention schedule for the records maintained in the system or by the project and records are not covered by a GRS, has a draft retention schedule been developed for the records used in this project or system?

Section 6.3(d) ☒ Yes ☐ No Have all applicable Treasury officials approved a draft retention schedule for the records used in this project or system?
Explanation of the Answers to Sections 6.3(a) through 6.3(d): In general, OFR SharePoint sites store and process various data. Data is derived from primary sources or source systems and then leveraged within SharePoint sites as necessary for a specific business purpose or need. Data is governed in accordance with the appropriate record schedule for the source data or source system. Data that is stored on OFR SharePoint sites will be managed under Records Control Schedule N1-056-03-10 (Records Common to Most Departmental Offices), specifically: • Item 1.b.2. Program files maintained by other DO components on or below the Deputy Assistant Secretary and Deputy General Counsel level (10-year temporary records) The foregoing Records Control Schedule will not apply to data stored on OFR SharePoint sites that is otherwise managed under an alternate, appropriately designated Records Control Schedule.

Section 6.4: E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act (hereinafter "FISMA") Security Assessment & Authorization process is required before a federal information system may receive Authority to Operate (hereinafter "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, if applicable, undergone a Security Assessment and Authorization and received Authority to Operate?
Explanation of the Answers to Sections 6.4 (a) and 6.4(b): At the time of drafting and publishing this PCLIA, the system was undergoing the SA&A process, which was expected to be finalized, and an ATO granted, in early April, 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?

Explanation of the Answer to Section 6.4(c): Access to data will be granted on an as-needed, least-privilege basis. Multiple layers of approval are required prior to granting access to data or systems at the OFR.

SharePoint, as implemented by the OFR, will rely on the application's security and governance model to allow site owners to manage content and security for sites under their responsibility. Acting in coordination with Division/Office SharePoint points of contact, site owners/administrators are responsible for monitoring and maintaining the content of their respective sites. The site owners/administrators ensure that information collected or placed into the OFR SharePoint sites are appropriate and in line with OFR data classification, security, and retention policies. Further, site owners are responsible for approving access to their sites and approving permissions associated with that access.

By policy, users of OFR's SharePoint environment are prohibited from publishing/storing sensitive or confidential files and information in areas of the portal not intended specifically for that purpose. Individual site owners are responsible for identifying and classifying all files and information published in their site in accordance with OFR's data classification procedures. Further, users are strongly discouraged from using SharePoint to store files or documents containing sensitive PII (e.g. SSNs, account numbers, etc.). By policy, individual sites are required to be reviewed on a regular basis by site owners to ensure only appropriate content is published and that access and security controls around such content is appropriate and in alignment with existing OFR policies and procedures.

Additionally, as a general matter, OFR has established a number of data handling procedures, quick references guides, and awareness campaigns to prevent misuse of OFR data, and employees are trained annually on the laws and policies governing the collection, use, maintenance and dissemination of PII. Employees are also required to agree to and acknowledge by signature "Rules of Behavior" governing appropriate use of OFR Information Technology and OFR information. OFR also works closely with the Treasury Office of Privacy, Transparency and Records on all issues related to PII.

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)?

Explanation of the Answer to Section 6.4(d): There are privacy risks associated with notice, and, to some extent, data minimization and accuracy, and data security. What follows is a discussion of each identified risk and the steps taken to mitigate the risk.

Individuals may not understand that their information is being collected or is being used within the OFR SharePoint sites.

These risks are most present where information is not collected directly from the individual or in cases where information is derived from source systems. To mitigate these particular risks, the OFR outlines its collection and use of such data in this PCLIA. For some information used by the system, individuals are able to input, add, or update their own information – for instance in their MySite public profile page. In such cases, individuals are afforded a notice (in addition to this PCLIA) in the form of a Privacy Notice within the OFR SharePoint environment, notifying them of the collection and use of their information.

There are risks associated with both data minimization and data quality. Again, these risks are most present when information is not collected directly from the individual, or is derived from source systems. OFR relies, where possible, on individuals to provide their information to help ensure that the data provided is current and not out of date. Further, where information can be obtained from authoritative sources, such as HRConnect, which provide correction opportunities, OFR has leveraged this data through automated processes. Generally, these two types of data make up the majority of PII in the OFR SharePoint environment. Finally, individuals have opportunities to update or correct this information through processes created to grant them access to the source system (when subject to the Privacy Act), or within the OFR SharePoint environment. With regards to data minimization, OFR limits its request and use of PII within OFR SharePoint sites to that which is relevant and necessary for clearly articulated OFR business processes. OFR regularly reviews its collection and use(s) of PII to ensure the appropriate information is captured for the identified business need. Further, by policy, users of OFR's SharePoint environment are prohibited from publishing/storing sensitive or confidential files and information in areas of the portal not intended specifically for that purpose. Individual site owners are responsible for identifying and classifying all files and information published in their site in accordance with OFR's data classification procedures. By policy, individual sites are required to be reviewed on a regular basis by site owners to ensure only appropriate content is published and that such content is in alignment with existing OFR policies and procedures.

Finally, there is a risk to the security and confidentiality of PII maintained in or processed by OFR SharePoint sites. As discussed in Section 6.4(c) above, access to data will be granted on an as-needed, least-privilege basis and in accordance with governance policies and procedures specific to the application.

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?
Explanation of the Answer to Section 6.4(e): In general, PII processed by or maintained on an OFR SharePoint site is not shared except as required by law or as outlined in applicable SORNs or similar notices and agreements that pertain to the source system and information processed by the system. Where information is shared with external, or internal parties, it is done so from the source system in accordance with OFR Information Security processes and policies, which meet the requirements outlined in Treasury policies and directives related to information security. The OFR SharePoint site is not the method by which such information is shared or transferred.

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?
Explanation of the Answer to Section 6.4(f): The system will not allow for the identifying or locating of individuals. However, the system will allow for monitoring of users of OFR SharePoint sites, for security, auditing, and functionality purposes.

Audit Trails
Section 6.4(g) ☒ Yes ☐ No Are audit trails regularly reviewed to ensure appropriate use, handling, and disclosure of PII maintained in the system or by the project inside or outside of the Department?

Explanation of the Answer to Section 6.4(g): OFR captures audit logs of employees, government contractors, and subcontractors using SharePoint sites to ensure their proper use. Monitoring is done in accordance with internal OFR information system audit and accountability procedures. Event logs and log management tools are secure and access is limited to authorized staff only. Audit logs and audit settings at the OFR may not be tampered with, deleted, or disrupted. Further, internal administrative policies and procedures govern appropriate use of the OFR's SharePoint sites and individual sites are required to be reviewed on a regular basis by site owners to ensure appropriate use in alignment with existing OFR policies and procedures.

Section 6.5: Section 508 of the Rehabilitation Act of 1973 Compliance

When federal agencies develop, procure, maintain or use Electronic and Information Technology (hereinafter "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 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)?

Compliance With the Rehabilitation Act
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?
Explanation of the Answer to Section 6.5(b): OFR has submitted the applicable VPAT associated with the SharePoint 2013 application to Treasury's Office of Privacy, Transparency and Records, as required by this assessment.

Section 7.0: Redress

Freedom of Information Act and Privacy Act Redress
Section 7.0(a) ☒ Yes ☐ No Does the agency have a published process in place by which individuals may seek information and redress under the Freedom of Information Act and Privacy Act?
Explanation for Answer in Section 7.0(a): The Treasury FOIA Regulations can be found at 31 CFR Part 1, Subpart A.

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?

Explanation of the Answer to Section 7.0(b): Information processed by or maintained in OFR SharePoint sites that is subject to the Privacy Act is not exempt 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 etc.)?
Explanation of the Answer to Section 7.0(c): Information processed or maintained in OFR SharePoint sites is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

Responsible Officials

Mario Nardoni
Associate Director, Analytic Systems
Office of Financial Research
U.S. Department of the Treasury

John Talbot
Chief Technology Officer
Office of Financial Research
U.S. Department of the Treasury

Ryan Law
Deputy Assistant Secretary for Privacy, Transparency, and Records
U.S. Department of the Treasury

Approval Signature

John R. Talbot [redacted]
Digitally signed by John R. Talbot
Date: 2016.09.20 11:07:15 -04 00

John Talbot
Chief Technology Officer
Office of Financial Research
U.S. Department of the Treasury

Mario A. Nardoni [redacted]
Digitally signed by Mario A. Nardoni
Date: 2016.09.12 14:43:03 -04'00'

Mario Nardoni
Associate Director, Analytic Systems
Office of Financial Research
U.S. Department of the Treasury


Digitally signed by Ryan A. Law
[redacted]
Date: 2016.09.20 15:39:19 -04 00

Ryan Law
Deputy Assistant Secretary for Privacy, Transparency and Records
U.S. Department of the Treasury