Privacy and Civil Liberties Impact Assessment
for the Office of Financial Research Analytical Environment (OFRAE)

March 3, 2016

Reviewing Official
Helen Goff Foster
Deputy Assistant Secretary for Privacy, Transparency, and Records
Department of the Treasury

Bureau Certifying Official
Wesley Fravel
Senior Information Security Specialist - Privacy
Office of Financial Research
Bureau 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 the how information is maintained, used and shared;
(4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and
(5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

This PCLIA is for the OFR's Analytical Environment (OFRAE). The OFRAE was previously documented in the Privacy Impact Assessment (PIA), Office of Financial Research Analytical Environment Privacy Impact Assessment, published in October 2014. OFR is conducting this revised PCLIA to evaluate new privacy implications associated with introducing additional IT capabilities to the OFRAE.

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 "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.

---

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 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.)"

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 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

The OFRAE is a foundational system that supports the OFR's mission of improving the quality, transparency, and accessibility of financial data and information. The OFRAE provides core and critical information technology support and services to OFR hosted applications and databases. The main components of the OFRAE are the:

- Security Environment
- Server Environment
- Virtual Desktop Environment (VDI)
- Data Environment

- Network Environment
- Application Environment

The OFRAE is designed to host applications and databases which process information, including PII, and to support transport and file storage of such information.

Per OFR's internal security and other assessment processes, and in accordance with Treasury policy and best practices, certain applications and databases hosted on the OFRAE are covered by their own separate PCLIAs when it is determined that those systems pose unique risks to personal privacy. Where applicable, those PCLIAs have been referenced in this document.

Section 3.1: System/Project Description

The OFRAE is the support structure and day-to-day working environment for OFR's employees, and other personnel including contractors, consultants, agents, detailees, interns, and business partners. The OFRAE enables the OFR to provide timely rigorous risk and stability analyses. In addition, it provides sufficient flexibility to support the continually evolving understanding of system risk and the changing needs for research and analysis.

The primary purpose of this revised PCLIA is to account for: (i) the transition of certain technical services from the Treasury Departmental Offices (DO) Office of the Chief Information Officer (OCIO) to the OFR; (ii) the introduction of two new technical services; and (iii) procured and acquired datasets which contain PII.

The technical services required by OFR employees transitioned from OCIO to OFR include: the provision and management of end point devices such as mobile devices and laptop computers; email services; and remote access capabilities. In addition, OFR is also introducing a variety of new technical capabilities and enhancements for users of the OFRAE and internal OFR systems.
In addition to the above services, OFR has either acquired or procured datasets containing PII which are used by staff in their research and analysis efforts. These datasets are primarily managed within the OFRAE Data Environment.

OFR End Point Devices (Mobile Devices/Laptop Computers)

OFR transitioned from OCIO-issued and managed endpoint devices (i.e., mobile devices and laptop computers) to OFR-issued and managed devices. OFR's chosen desktop and mobile solutions provide increased performance in a form factor that meets the unique requirements of OFR staff while leveraging existing OFRAE security controls and configurations. Further, support for endpoint devices is managed through a dedicated OFR Help Desk capability.

OFR (ofr.treasury.gov) Email Services

OFR leveraged existing infrastructure capabilities provided by the OFRAE to transition e-mail services from the DO Exchange environment to a new Exchange environment established and managed within the OFRAE.

OFR Remote Access Capability

OFR facilitates secure remote access to the OFRAE for authorized users through the OFR Remote Access Capability. This capability allows users to access their OFRAE desktops and applications remotely via the internet.

OFR PIV Data Synchronization

The OFR previously leveraged Treasury DO's Personal Identity Verification (PIV) Data Synchronization (PDS) platform for the creation of OFRAE user accounts, the issuance of user IDs and email addresses, and the automated initiation of the PIV issuance process. With the transition of IT services, OFR is now responsible for these automated processes. Upon receiving notice of a new onboarding OFR employee, the OFR's PDS takes PII and other related data about the new employee and uses this information to create a user account, a User Provision Name, and email address for the employee. This information is then routed back to Treasury's Human Resources Connect (HRConnect) system to populate the new employee's record and begin the PIV card provisioning process. OFR has executed an Interconnection Security Agreement (ISA) for the secure transfer of this data from and to Treasury, across the OFRAE.

OFR Acquired/Procured Datasets

Finally, OFR has attained several new datasets in support of its research mission, which are processed by applications and databases within the OFRAE. In general, these data are used for trend analysis in the aggregate. Research is done across the datasets to identify macro-level risks and trends in financial markets. These datasets and their uses in support of specific research initiatives and questions are further described in Section 4.3 of this PCLIA. Where these datasets were not accounted for in the last version of this PCLIA, or in a separate PCLIA specific to the application which processes them or the project which they support, and where they include PII, they have been included for discussion in this PCLIA. A complete list of these datasets is included in the table below.

Dataset	Description
Bankscope	A proprietary, comprehensive, global database of banks' financial statements, ratings and intelligence. Includes names of directors and business contact information for banks.
Equilar Executive Compensation Data	Proprietary dataset that includes information about total executive compensation packages of the top officers at publicly traded companies and nonprofit organizations. Includes the full name of the executive as well as their compensation.
Financial Industry Regulatory Authority (FINRA) Form Advisor Disclosure Vette (ADV) Data	Data from the uniform form used by investment advisers to register with both the Securities and Exchange Commission (SEC) and state securities authorities. Includes names and business contact information (address, email, phone number) of industry figures (investment advisors).

OpenCorporates	Publicly available dataset that includes basic, publically available, data from company registers, including the names and directors of company owners, as well as official mailing addresses for such companies.
Factiva	Trade, publication/journals which may include PII such as author names, that is germane to the content of the information.
SEC Form Private Fund (PF) Data	Data from the form used private fund advisers to report regulatory assets under management to the Financial Stability Oversight Council. The form is managed by the SEC and includes names of investment advisors. More information on Form PF is available at https://www.sec.gov/about/forms/formpf.pdf.
HRConnect Data	Data from the Treasury's HRConnect system, which provides the OFR with names, titles, and basic business contact information (duty station address, phone number) related to OFR employees and contractors for population into user accounts within OFRAE and other related onboarding functions, such as creating and assigning email addresses.

This PCLIA does not address information in the OFR's Constituent Relationship Management (CRM) system. While the CRM is operated in the Application environment of the OFRAE, OFR has chosen to address the system and the PII it processes in a separate Privacy and Civil Liberties Impact Assessment for the CRM.

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

The OFRAE hosts applications and databases which process PII and supports the transport and file storage of such information. PII processed by OFRAE-hosted applications and databases, or transported using the OFRAE generally consists of one of three "types" of collections, which includes: 1) names, business contact information, and other limited HR used to facilitate daily business functions of the OFR, like managing employee workloads, facilitating communication with employees, or granting access to OFRAE-hosted or supported applications and databases; 2) names and basic contact information of members of the public who have partnered with the OFR in support of OFR's research mission, in order to coordinate related efforts, such as OFR federal advisory committee meetings, or to publish research papers and reports; and 3) publically available and proprietary information used in support of the OFR's research-based mission, which where possible, has been stripped of direct identifiers.

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): Information processed by the OFRAE, implicates a variety of information, including PII, some of which is subject to the Privacy Act. In general, PII processed by the OFRAE that is subject to the Privacy Act includes: - Data provided from Treasury's HRConnect system or collected directly from OFR employees and contractors that is used to create user accounts and grant authorized users access to applications hosted on or supported by the OFRAE, or to conduct other similar routine administrative functions. - Data provided from the SEC's Form PF via FINRA through the transmission of Form PF to the OFR. For data acquired from Treasury's HRConnect system and the SEC's Form PF, PII was collected by the Treasury Department and SEC, respectively, in accordance with rules, procedures, and processes specific to those agencies, including an assessment by the agency responsible for the original collection and maintenance of these records, to determine which PII types are relevant and necessary. While OFR does not oversee these assessments, it does limit its request for and collection of information from other Federal entities to that which is relevant and necessary for OFR's purpose(s). More information about the collection and processing of PII included in Treasury's HRConnect system is available in the Privacy and Civil Liberties Impact Assessment for the system. For data collected to grant OFR employees, contractors, and authorized users access to applications and databases hosted on or supported by the OFRAE, such information is governed in accordance with the Treasury System of Records Notice, 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 applications and databases hosted on the OFRAE. OFR regularly reviews its user access processes and collections of PII to ensure the appropriate information is captured to ensure access to and security of OFR systems. Finally, some data collected as normal business operations related to engaging members of the public who partner with the OFR in support of its research mission, is subject to the Treasury System of Records Notice, Treasury.017 – Correspondence and Contact Information.

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* **Such information has been stripped of direct-identifiers or aggregated and used for trend analysis to identify macro-level risks and trends in financial markets.*	☒ Group/Organization Membership
☒ Birth Date	☒ Race/Ethnicity* ** Such information has been stripped of direct-identifiers or aggregated and used for trend analysis to identify macro-level risks and trends in financial markets.*	☐ Military Service Information
☒ 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* **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.*	☐ Religion/Religious Preference	☐ References or other information about an individual's friends, associates or acquaintances.
☒ Personal Financial Information (including loan information)* ** In general, such information has been stripped of direct-identifiers or aggregated and used for trend analysis to identify macro-level risks and trends in financial markets. In*	☐ Passport Information	☐ Global Positioning System (GPS)/Location Data

limited cases, OFR may have access to compensation information about specific individuals through the Equilar dataset as described in this PCLIA.		
☐ 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 and contractors, 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): Form PF filer's business mailing address, email address, telephone number and other contact information for SEC registrants made available for public search by the SEC.*
☒ Other (please describe): SEC 801 number, National Futures Association (NFA) ID, and Large Trader ID as made available by SEC registrants on Form PF.	☒ Other (please describe): "Public profiles" of executives or board members as reported by Equilar.	

Identifying Numbers Assigned to Individuals	
☐ Full Social Security number	☐ Personal Bank Account Number
☐ Truncated Social Security Number (e.g., last 4 digits)	☐ Health Plan Beneficiary Number
☒ Employee Identification Number *As part of the onboarding process described in this PCLIA, OFR receives an identification number (GUID) specific to an employee's record within the HRConnect System – this number, is the employee's ID number in the HRConnect System and is used to facilitate population of the employee's user account, establish their username and email address, and begin the PIV provisioning process.*	☐ 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 and contractors on administrative documents such as training requests, letters, or certificates.*	☐ Vascular scans
☐ Fingerprints	☒ Photos* **To include OFR employees and contractors and individuals who attend OFR-sponsored events.*	☐ Retina/Iris Scans
☐ Palm prints	☐ Video	☐ Dental Profile
☐ Voice audio recording	☐ Scars, marks, tattoos	☐ DNA Sample or Profile
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe):

Specific Information/File Types 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 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	☒ 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): ____	☐ Other (please describe): _____
☐ Other (please describe): _____	☐ Other (please describe): _____

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

A large portion of information processed by the OFRAE is retrieved from third-party sources, and is not collected directly from individuals. Third-party sources providing data include commercial data sources, public data sources, and other State and Federal agencies.

Information collected directly from individuals that is processed by the OFRAE is generally limited to:

- Name, contact, and other similar limited data about OFR employees and contractors used to facilitate daily business functions of the OFR.
- Name and basic contact information of members of the public who have chosen to engage or partner with the OFR on its research mission.

Generally, this information is collected through informal means, such as in-person contacts, or via email. In other cases, this information was originally collected directly from individuals by the source system, and in accordance with rules and procedures specific to those systems and agencies; for example, HRConnect, or the SEC's Form PF.

The OFR also receives information from Treasury's HRConnect system, which provides the OFR with basic business contact information related to OFR employees and contractors for creating user

accounts within OFRAE and other related onboarding functions provided by the OFR's PDS. Information from the HRConnect system is collected in accordance with procedures specific to that system as outlined in the HRConnect Privacy and Civil Liberties Impact Assessment.

Information not collected directly from the individual that is processed by the OFRAE includes:

- Datasets, stripped of direct identifiers or otherwise aggregated, and used for trend analysis to identify macro-level risks and trends in financial markets, as part of OFR's overall research mission.
- Datasets which may include direct identifiers and are also used for trend analysis or to identify macro-level risks and trends in financial markets in support of OFR's research mission.

Some of this data is derived from publically available sources, some is provided by other Federal entities, while other data is proprietary in nature. All such data is used in support of the OFR's research-based mission, and generally includes things like mortgage, transactional, loan information, demographic, or similar data, which has been either stripped of direct identifiers or provided in aggregate to reduce the risk posed to personal privacy. In unique cases, OFR may receive direct identifying information in support of its research mission (i.e. Equilar data). Data obtained for research and processed through the OFRAE includes:

- Data obtained from the Financial Industry Regulatory Authority (FINRA), as directed by the Securities and Exchange Commission (SEC). FINRA is a private corporation that performs financial regulation of member brokerage firms and exchange markets that collect Form PF data on behalf of the SEC. Filers submit Form PF through the Private Fund Reporting Depository (PFRD). FINRA is the developer and operator of the PFRD system, which was developed according to the requirements of the SEC.
- Form PF data, which is used by the OFR to better understand the role hedge funds play in the financial system to monitor risks in the private fund industry, and to research threats to financial stability. Advisors for hedge funds and other private funds with more than $150 million in assets under management have been electronically filing annual portfolio information through the SEC's Form PF since July 2012. The annual and quarterly filings of Form PF provide OFR with a new window into the activities of private funds. OFR use of Form PF data is governed by an agreement between the OFR and the SEC, as well as a Memorandum of Understanding signed by all of the Financial Stability Oversight Committee (FSOC) member agencies including OFR ("FSOC MOU").
- Executive compensation data from Equilar, Inc., a commercial data provider. Equilar creates data products and sells third parties such as OFR, licenses to an Equilar product which includes information about total executive compensation packages of the top officers at publicly traded companies and nonprofit organizations. OFR receives the full name of the executive whose compensation data is collected by Equilar. Equilar collects this data from publically available sources such as annual corporate filings with the SEC, filings through the Department of the Labor, and from surveys completed by executives.
- Bankscope data, which includes limited biographical information of public figures in the financial industry.

- Factiva news, data, and analysis products, which includes limited biographic information of authors of articles and stories found in industry trade publications.
- OpenCorporates data, which includes the names and address information of public figures associated with corporations.

Each of these data products is discussed further in Section 3.1 of this PCLIA.

OFR Employees/ Contractors	Members of the Public Who Engage with OFR on Research Mission	Treasury HRConnect	Data received from third parties (other agencies or vendors) in support of OFR's research mission
Specific PII identified in Section 4.2 that was acquired from this source: – Employee, contractor, consultant name – Business Contact Information (phone, email address, duty location) – Title – Supervisor – Duty status – Emergency contact information, including limited personal contact information – Audit log and security monitoring information – Personnel files – Security clearance information – Signatures – Photos – Resumes/CVs	**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, etc. – Resumes and CVs of board members and researchers conducting research on behalf of OFR; – Limited audit log and security monitoring information for individuals accessing the OFR public network at its headquarters	**Specific PII identified in Section 4.2 that was acquired from this source:** – Employee, contractor, consultant name – Business email address – Business phone number – Business address – Title – Duty status/location – OFRAE User Provision Account names – Employee GUID	**Specific PII identified in Section 4.2 that was acquired from this source:** – Full name of investment advisors required to register with SEC via Form PF; – Business mailing address, email address, telephone number as provided on Form PF; – NFA ID, SEC 801 number, and Large Trader ID as provided on Form PF; – "Public profiles" as reported by Equilar; – Names and contact information of public figures or members of industry from proprietary (Bankscope) and public (OpenCorporate) data sources; – Names of individuals who author stories or articles in industry

			trade publications through Factiva; – Publically available and proprietarily sourced data includes limited PII, such as loan level information or race/demographic information and has been stripped of direct-identifiers or aggregated, and is used for research purposes
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):**	**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): _____	☐ 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): _____	☐ 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.	☐ 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.	☒ 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	☒ Accessed and downloaded or otherwise acquired via the internet
☒ Email	☒ Email	☐ Email	☐ Email
☒ Scanned documents uploaded to the system.	☒ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.
☐ Bulk transfer	☐ 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).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
☒ Fax	☒ 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	☐ Extracted from notes of a phone interview or face to face contact
☒ Other: Please describe: Acquired through employee's use of OFRAE-hosted or supported applications and databases by security, auditing, and other similar logging methods.	☐ Other: Please describe: _____	☒ Other: Please describe: Data is acquired by OFR's PDS to create user accounts, email address/accounts, and perform similar onboarding functions. This occurs by the PDS sending an XML SOAP request to HRConnect for relevant information.	☐ Other: Please describe: _____
☐ Other: Please describe: _____	☐ 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 by the OFRAE is not collected directly from individuals and is retrieved from other sources, including commercial data sources, public data sources, and other State and Federal agencies.

Information collected directly from the individual that is processed by the OFRAE is generally limited to name, contact, and other similar limited data about OFR employees and contractors used to facilitate daily business functions of the OFR, as well as names and basic contact information of members of the public who have chosen to engage or partner with the OFR on its research mission. Generally, this information is collected through informal means, such as in-person contacts, or via email.

Other PII processed by the OFRAE that is subject to the Privacy Act is not collected directly by the OFR, and includes data provided from Treasury's HRConnect system and the SEC's Form PF. PII included 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): The OFRAE does not collect, maintain or request Social Security numbers (SSN).

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): The OFRAE does 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.

Information, including PII, processed by the system is used for research or administrative purposes. The PII usage is consistent with the OFR's mission because it allows the agency to provide rigorous risk and financial stability analyses. In addition, it provides sufficient flexibility to support the continually evolving understanding of systemic risk including new and emerging trends in financial research and analysis.

The OFRAE hosts or supports applications and databases which process PII and supports the transport and file storage of such information. PII processed by OFRAE-hosted applications and databases, or transported using the OFRAE is limited to that which is necessary for one of three functions related to research or administration:

- PII necessary to facilitate daily business functions of the OFR, like managing employee workloads, facilitating communication with employees, or granting access to OFRAE-hosted or supported applications and databases. This includes PII such as employee names, titles, email addresses, phone numbers, and other business contact information, emergency contact information, including personal phone or email addresses, and other HR related data, such as performance data;
- PII used in support of OFR's research mission, in order to coordinate related efforts, such as OFR federal advisory committee meetings, or publishing research papers and reports. This includes names and professional contact information, CVs, educational information, and professional association information for individuals who are engaged in research projects with the OFR, supporting OFR research efforts, or serving on an OFR-sponsored board or advisory committee;
- PII used in support of OFR's research initiatives, including:
    - Publically available and proprietary information used in support of the OFR's research-based mission, which has been stripped of direct identifiers, but may include data which is linkable to a specific individual, such as loan-level data, ZIP codes, aggregate demographic information, etc.; and
    - PII collected from other Federal and State agencies and proprietary sources used in support of OFR's research initiatives.

Sections 4.3 and 3.1 provide additional information on each of these data.

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 by the OFRAE 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 by the OFRAE to conduct "data-mining" activities as that term is defined in the Implementing the 9-11 Commission Act.

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

Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

The Privacy Act requires that federal agencies: "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 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 by the OFRAE 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 the OFRAE that is 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 by OFRAE 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): The OFR purchases or acquires electronic datasets from third party vendors, public sources, and other State and Federal agencies, and may merge such data to form aggregate datasets for research purposes. While these datasets may contain PII, they are generally stripped of any direct-identifiers and are used for trend analysis in the aggregate rather than making determinations about specific individuals. Research is done across the datasets to identify macro-level risks and trends in financial markets, not to identify or make determinations about individuals.

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 by the OFRAE 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): Prior to obtaining a dataset, data standards are established which specify the format in which the OFR expects to receive the data that it has procured or acquired. Extract, transform, and load (ETL) processes are developed such that accuracy and completeness are validated during the ETL process to verify that data has been received according to procurement and data management specifications. ETL processes are performed when data is received from a third party vendor to extract the data is needed for financial research purposes, transform the data in the required format for loading into OFR systems, and loading the standardized format into OFR systems for further analysis. ETL processes are developed such that if data is received in an unexpected format or with unexpected data included, the ETL process will fail and coordination with the vendor will be required to move forward with the data intake process.

Access to the OFRAE is granted through the approval process outlined in the OFR Access Control Procedures. In general, individuals make access requests by submitting the necessary information through an electronic workflow.

For data that is received from Treasury HRConnect regarding contact information, this information is 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.

As outlined above, information processed by the OFRAE is not 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): PII processed by the OFRAE is shared with third parties as outlined in the applicable SORN or as required by law. In general, PII maintained or processed by the system is not collected directly from individuals, but in cases where it is collected directly by OFR or Treasury, processes exist to disseminate such updates to appropriate internal information sharing partners. For example, OFR employees may update their information either directly through the system or by contacting an HR representative. In cases where information is not collected directly from the individual, processes exist through the source system for the information (where feasible and appropriate) and not through the OFRAE, which is only a vehicle by which such information is accessed. Finally, PII which OFR receives from another Federal agency is updated by the agency which provided the PII.

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): PII processed by the OFRAE may be shared with other components of Treasury on a need-to-know basis, for example, with representatives from Treasury's human resources, or with FSOC or FSOC member agencies. Treasury and OFR have procedures and policies in place which govern both the sharing and use of such information.

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; FSOC
Purpose of the Sharing	OFR staff and FSOC may request access to data maintained by OFR for purposes consistent with OFR's research mission and statutory authority. Internal data access requests are reviewed and approved in accordance with OFR user access policies and guidelines. Data shared internally is based on specific, discrete user access requests and such access is based on a demonstrable need-to-know in support of a specific business function or request.
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." Use of such information is governed by the agreement, license, or contract applicable to the dataset or other information.
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. In addition, data shared between OFR and FSOC, including FSOC member agencies is subject to the restrictions contained in the FSOC MOU as well as the provisions of the applicable contract, lease, or license.
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	Each of the datasets referenced above are subject to an applicable 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.
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	The method of PII transfer is based on the nature of the request and the receiving office or portion of Treasury. Generally data is transferred via secure electronic means.

device/email fax/other (please describe if other)	

Explanation for Responses in the Internal Information Sharing Chart: Each of the datasets referenced above are subject to information sharing agreements, memoranda of understanding or agreement, or contractual agreements stipulating use of the data for the stated and intended purpose. For the most part these agreements do not specifically stipulate restrictions related to sharing or use of PII, but instead focus on disclosure of proprietary information. The exception is the Information Sharing Agreement governing OFR's connection to HRConnect for facilitating the creation of user accounts, which stipulates that OFR use PII only for the intended purpose and limit access to individuals who demonstrate a bona-fide need-to-know.

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 processed by the OFRAE is not shared with agencies, organizations, or individuals external to Treasury except as required by law or as outlined in applicable SORNs that pertain to 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): PII processed by the OFRAE is only shared with external information sharing partners as required by law, or as outlined in the specific SORN which governs a particular information collection processed by the OFRAE or an OFRAE application or database.

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.

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): Any such sharing would be governed by the terms of the FSOC MOU and the applicable contract, license, or other agreement governing use of the data. However, please note that PII processed by the OFRAE is only shared with external information sharing partners as required by law, or as outlined in the specific SORN which governs an information collection processed by the OFRAE or in an OFRAE application or database. Section 5.3(c) includes more information on agreements governing PII processed by the OFRAE.

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): Information procured or otherwise attained from third parties, including proprietary sources and other Federal and State agencies are subject to the FSOC MOU and the applicable data agreements governing OFR's use and sharing of the data. Section 5.3(c) includes more information on agreements governing PII processed by the OFRAE.

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 the OFRAE is only shared with external information sharing partners as required by law, or as outlined in the specific SORN which governs the information collection processed by the OFRAE. Section 5.3(c) includes more information on agreements governing PII processed by the OFRAE.

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): PII processed by the OFRAE is only shared with external information sharing partners as required by law, or as outlined in the specific SORN which governs information collection processed by the OFRAE or in an OFRAE application or database.

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): Information processed by the OFRAE, implicates several System of Records Notices, including:

For data acquired from Treasury's HRConnect System, such data is managed in accordance with Treasury.001 – Treasury Payroll and Personnel System, 79 FR 183.

For data collected to grant OFR employees, contractors, and authorized users access to applications and databases hosted on or supported by the OFRAE, such information is governed in accordance with the Treasury System of Records Notice, Treasury.015 – General Information Technology Access Account Records (GITAARS), 80 FR 1988.

For data related to engaging members of the public who partner with the OFR in support of its research mission, which is subject to the Privacy Act, such information is managed in accordance with the Treasury System of Records Notice, Treasury.017 –Correspondence and Contact Information, 80 FR 34963.

Form PF data received from the SEC is subject to the SEC's SORN for those records.

Section 6.2: The Paperwork Reduction Act

The PRA requires OMB approval before a federal agency may collect standardized data from 10 or more respondents within a 12 month period. OMB requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of [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): Treasury Schedule "Records Common to Most" Items 1c and 18, as well as Treasury Guidance (TD) 80-07 and NARA GRS 6.1 govern non-personnel records processed by the OFRAE.

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): The OFRAE is categorized as a FIPS 199 moderate system and NIST 800-53 controls are configured in accordance with a FIPS 199 moderate baseline. The system was granted an Authority to Operate (ATO) effective 3/6/2014. The ATO expires on 3/6/2017.

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 through the approval workflow outlined in the OFR Access Control Procedures. Multiple layers of approval are required prior to granting access to data or systems at the OFR.

Access controls are enforced by the OFR Information Security Team. Only authorized personnel have access to monitoring tools. The central log management tool that OFR is utilizing enforces access controls. The OFRAE is categorized as a FIPS 199 moderate system and NIST 800-53 controls are configured in accordance with a FIPS 199 moderate baseline.

Further OFR has established a number of data handling procedures, quick references guides, and awareness campaigns to prevent misuse of OFR data.

Finally, 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 participation and notice.

Individuals may not understand that their information is being collected, and may have limited opportunities for correcting or amending their information.

These risks are most present where information is collected directly from the individual in order to grant access to a system or application housed on the OFRAE. To mitigate these particular risks, the 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. Further, individuals have opportunities to update or correct this information through processes created to grant them access to OFR resources, or through processes outlined in the HRConnect Privacy Impact Assessment and related System of Records Notice.

Information used by OFR for research purposes and received from third parties presents a similar, albeit lower level of risk. In these instances, OFR does not use such information to make determinations about specific individuals, instead such information are generally stripped of any direct-identifiers and are used for trend analysis in the aggregate. Research is done across the datasets to identify macro-level risks and trends in financial markets, but not related to individuals. As such, while data accuracy is less relevant, notice opportunities may

be limited. That said, to foster transparency and reduce residual risk, OFR is outlining its collection and use of such data in this PCLIA.

Finally, as referenced above, for information subject to the Privacy Act, individuals are afforded opportunities to access and correct their information as outlined in the applicable SORN for each system or dataset.

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): PII processed by the OFRAE is not shared with external parties unless required by law or as authorized under the applicable SORN. Where information is shared with external, or internal parties, it is done so in accordance with OFR Information Security processes and policies, which meet the requirements outlined in Treasury policies and directives related to information security.

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 does not allow for the identifying or locating of individuals. However, the system does allow for monitoring of users of the OFRAE, 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): The OFRAE captures audit logs of employees, government contractors, and subcontractors using the OFRAE to ensure its 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. Any changes must be approved by the OFR Change Control Board (CCB) through a formal review of a configuration change request.

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 conducted and/or reviewed Voluntary Product Assessment Templates for the following new technologies associated with the OFRAE: – Endpoint devices (mobile devices and laptops) – Remote capability, including VDI (operating system and Citrix plug-in). OFR is working to address those product functions which only partially support applicable 508 standards.

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 the OFRAE 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 by the OFRAE is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

Responsible Officials

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

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

Helen Goff Foster
Deputy Assistant Secretary for Privacy,
Transparency, and Records
U.S. Department of the Treasury

Approval Signature

Digitally signed by John R. Talbot
John R. Talbot [redacted]
Date: 2016.03.07 15:49:12 -05'00'

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

Digitally signed by Helen g. Foster
Date: 2016.05.23 08:54:13 -04'00'

Helen Goff Foster
Deputy Assistant Secretary for Privacy,
Transparency and Records
U.S. Department of the Treasury

Digitally signed by Mario A. Nardoni
Mario A. Nardoni [redacted]
Date: 2016.03.04 08:51:32 -05'00'

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