Privacy and Civil Liberties Impact Assessment
for the

External Facing Web Applications
Office of Foreign Assets Control (OFAC) Consolidated Technology System (OCTS)

July 14, 2020

Reviewing Official

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

Section 1: Introduction

PCLIAs are required for all systems and projects that collect, maintain, or disseminate personally identifiable information (PII). The system owner completed this assessment pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget (OMB) Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before: (1) developing or procuring information technology (IT) systems or projects that collect, maintain or disseminate PII from or about members of the public, or (2) initiating a new collection of information that: (a) will be collected, maintained, or disseminated using IT; and (b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons (not including agencies, instrumentalities, or employees of the federal government).

It is the policy of the Department of the Treasury ("Treasury" or "Department") and its Bureaus to conduct a PCLIA when PII is maintained in a system or by a project. 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.

Section 2: System Overview

Section 2.1: System/Project Description and Purpose

The Department of the Treasury Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on United States foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists that include individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." SDNs' assets are blocked and U.S. persons may not engage with them in trade or financial transactions or other dealings unless authorized by OFAC or expressly exempted by statute. The term "U.S. persons" includes all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S incorporated entities and their foreign branches. In the cases of certain programs, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by U.S. companies also must comply. OFAC makes many of its sanctions list files available to the public by anonymous file transfer protocol (FTP), ftp://ofacftp.treas.gov.

OFAC Consolidated Technology System (OCTS) is a set of interconnected applications sharing common functionality under OFAC internal management control. OCTS components are web based applications that reside on servers hosted at the Bureau of the Fiscal Service (FS) in Parkersburg, West Virginia. OCTS is a child application under the Treasury External Facing Web Application General Support System. OCTS is comprised of the following OFAC applications:

- *This Sanctions List Search ("Sanctions Search") – All financial institutions and persons in the U.S. are required to block financial transactions that are linked to individuals, entities, and vessels that are identified in the SDN list or react appropriately to transactions that potentially violate one of the OFAC country-specific programs. Sanctions Search is an application designed to facilitate the use of the SDN and blocked persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the List of persons identified as blocked solely pursuant to Executive Order (E.O.) 13599, the Non-SDN Iran Sanctions Act List, the Part 561 list, the Sectoral Sanctions Identifications List and the Non-SDN Palestinian Legislative Council List. SDN data is derived from several sources, including open source/internet research, news articles, Federal intelligence data, Federal law enforcement data and data provided per international agreements and alliances with foreign governments. SDN data is unclassified and information related to foreign nationals, US citizens, Lawful Permanent Residents (LPRs), and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also contains individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. In addition to returning results that are exact matches (when the match threshold slider bar is set to 100%), Sanctions List Search can also provide a broader set of results using fuzzy logic. This logic uses character and string matching as well as phonetic matching. Only the name field of Sanctions List Search invokes fuzzy logic when the tool is run. The other fields on the tool use character matching logic.*

- *Automated Blocking and Reject Reporting System High Volume (ABaRRS HV) – ABaRRS HV is a customized, public-facing, web-based interface that electronically tracks and stores information regarding fund transfers and property transactions that financial institutions blocked or rejected in accordance with U.S. economic sanctions policy. ABaRRS HV is the only OCTS component with registered external users. ABaRRS HV users are primarily members of various financial institutions that are required to submit blocked and rejected reports to OFAC via the ABaRRS HV website. https://abarrshv.ofac.treas.gov. Although all US persons are required to reject and report certain transactions, ABARRS HV data is provided to OFAC primarily by financial institutions reporting blocked or rejected transactions (e.g., wire transfers, trade finance, securities, checks, foreign exchange, and goods or services) as required by law. The public interface allows financial institutions and other members of the public to submit reports of blocked property and rejected fund transfer reports using a web based form for single report submission and batch report upload using an extensible markup language (xml file). As transactions are imported into ABaRRS HV, they are reviewed and investigated by OFAC personnel to determine if any transaction appears to be unusual or if further action is necessary. Transactions reported include PII related to US. citizens and LPRs.*

- *OFAC Administrative System for Investigations and Sanctions (OASIS) – is OFAC's internal case management system. OASIS is a customized web-based repository for all OFAC correspondence and subsequent unclassified casework (in the areas of licensing, enforcement, compliance, Freedom of Information Act (FOIA), Office of Global Targeting (OGT) and Specially Designated Nationals (SDN)). It consists of a set of applications called modules. The modules are tailored for the work processes of each group within OFAC. Each respective business unit has functionality to enter, review, track, assign, search and report on case related information. Information regarding foreign nationals, US citizens, LPRs, and*

companies owned or controlled by, or acting for or on behalf of, targeted countries is collected and used in OASIS for the purpose of carrying out OFAC's objectives.

- *Public Facing Licensing – Public Facing Licensing is a customized web-based information system that supports OFAC's requirements for issuing a license to the public. The license is an authorization from OFAC to engage in a transaction that otherwise would be prohibited. PII is collected and used to issue licenses to the public for Cuba travel, release of blocked wire transfers, export of agricultural commodities, medicine, or medical devices to Sudan or Iran (pursuant to the Trade Sanctions Reform and Export Enhancement Act of 2000), or other applications for interpretive/transactional guidance. Licenses applications that would be submitted with this application are:*
  - *Application for authorization to travel to Cuba under a specific license (should the travel be authorized pursuant to a general license, do not submit an application for a specific license.)*
  - *Application for the release of a wire transfer blocked at a U.S. financial institution*
  - *Application for a specific license or interpretive guidance in all other circumstances ("Transactional")*
  - *Application to export agricultural commodities, medicine, or medical devices to Sudan or Iran pursuant to the Trade Sanctions Reform and Export Enhancement Act of 2000.*

OCTS users include Treasury OFAC employees, designated consultants and contractors performing OCTS end user and application-specific system administration, development, and maintenance functions. In addition to the above mentioned users, OCTS users consist of approved external financial institutions accessing ABaRRS HV, public facing licensing applicants, and general public searching/reading the SDN List.

1. ☐ A PCLIA is being done for this system for the first time.
2. ☒ This is an update of a PCLIA previously completed and published under this same system or project name. The date the earlier PCLIA *was published was March 15, 2013*
3. ☐ This is an update of a PCLIA previously completed and published for a similar system or project that is undergoing a substantial modification or migration to a new system or project name. The name of that previous PCLIA was *[Name the PCLIA here]* and the date of its publication was *[provide **here** the date the earlier PCLIA was published]*.

Section 2.2: Authority to Collect

Federal agencies must have proper authority before initiating a collection of information. The authority is sometimes granted by a specific statute, by Executive order (EO) of the President or other authority.

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

The information may also be collected pursuant to a more general requirement or authority. All Treasury systems and projects derive general authority to collect information from:

- *5 U.S.C. 301 – Authorizing the Secretary to prescribe regulations for the operations of the department, conduct of employees, distribution and performance of its business, the custody, use, and preservation of its records, papers, and property.*
- *31 U.S. Code § 321.General authority of the Secretary*

Section 2.3: Privacy Act Applicability; SORN Requirement

Under certain circumstances, federal agencies are allowed to exempt a system of records from certain provisions in the Privacy Act. This means that, with respect to information systems and papers files that maintain records in that system of records, the agency will not be required to comply with the requirements in Privacy Act provisions that are properly exempted. If this system or project contains records covered by the Privacy Act, the applicable Privacy Act system of records notice(s) (SORNs) (there may be more than one) that cover the records in this system or project must list the exemptions claimed for the system of records (it will typically say: "*Exemptions Claimed for the System*" or words to that effect).

Section 2.3(a)

1. ☐ The system or project does ***not*** retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. A SORN is ***not*** required with respect to the records in this system.
2. ☒ The system or project ***does*** retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. A SORN ***is*** required with respect to the records in this system.
3. ☒ A SORN was identified in the original PCLIA and a determination was made during this current PCLIA update that modifications ☒ were required to that SORN. The applicable SORN is: ***DO .120*** - *Records Related to Office of Foreign Assets Control Economic Sanctions - 81 FR 78298(Nov. 7, 2016)*
4. ☐ A SORN(s) was not identified or required in the original PCLIA, but a determination was made during this current PCLIA update that a SORN(s) is now required. The applicable SORN(s) is:
5. ☐ A SORN was published and no exemptions are taken from any Privacy Act requirements.
6. ☒ Exemptions are claimed from the following Privacy Act provisions in the applicable SORN(s): "*Records in this system related to enforcement, designation, blocking, and other investigations are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). See 31 CFR 1.36.*"

Section 3: Information Collection

Section 3.1: 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 accomplished by statute or by executive order of the President." 5 U.S.C. § 552a (e)(1). It allows federal agencies to exempt records from certain requirements (including the relevant and necessary requirement) under certain conditions. 5 U.S.C. §552a (k). The proposed exemption must be described in a Notice of Proposed Rulemaking ("NPRM"). In the context of the Privacy Act, the purpose of the NPRM is to give the public notice of a Privacy Act exemption claimed for a system of records and solicit public opinion on the proposed exemption. After addressing any public concerns raised in response to the NPRM, the agency must issue a Final Rule. It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final Rule process.

Section 3.1(a) *Exemption Claimed from this Requirement?*

1. ☐ The PII maintained in this system or by this project is ***not*** exempt from 5 U.S.C. § 552a(e)(1), the Privacy Act's requirement that an agency "*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 accomplished by statute or by executive order of the President."

2. ☒ OFAC followed the proper regulatory procedures to exempt the PII maintained in this system from 5 U.S.C. § 552a as allowed by Sections (k)(1) and (k)(2) of the Privacy Act.

Section 3.1(b) *Continuously Assessing Relevance and Necessity*

1. ☐ The PII in the system is not maintained in a system of records. Therefore, the Privacy requirements do not apply. *[Explain **here** what you do to ensure relevance and necessity despite the fact that the Privacy Act does not apply].*
2. ☐ The PII in the system is maintained in a system of records, but the agency exempted these records from the relevance and necessity requirement.
3. ☒ The system owner conducted an assessment prior to collecting PII for use in the system or project to determine which PII data elements and types (see Section 3.2 below) were relevant and necessary to meet the system's or project's mission requirements during this analysis *In conducting the "relevance and necessity" analysis that is documented in this PCLIA, the system owner reevaluated the necessity and relevance of all PII data elements and determined that they are still relevant and necessary. Every time this PCLIA is updated, this ongoing assessment will be revisited. If it is determined at any time that certain PII data elements are no longer relevant or necessary, the system owner will update this PCLIA to discuss how the data element was removed from the system and is no longer collected.*
4. ☒ With respect to PII ***currently*** maintained (as of the time this PCLIA is being done) in the system or by the project, the PII ☒ is limited to only that which is relevant and necessary to meet the system's or project's mission requirements. *During the PCLIA process, the system always undergoes a review to ensure the continuing relevance and necessity of the PII in the system.*
5. ☒ With respect to PII maintained in the system or by the project, there ☒ is a process in place to continuously reevaluate and ensure that the PII remains relevant and necessary. *During the PCLIA process, the system always undergoes a review to ensure the continuing relevance and necessity of the PII on the system. If a determination is made that particular PII is no longer relevant and necessary in between scheduled PCLIA updates, this PCLIA will be updated at that time.*

Section 3.2: PII and/or information types or groupings

The checked boxes below represent the types of information maintained in the system or by the project that are relevant and necessary for the information system or project to fulfill its mission. PII identified below is used by the system or project to fulfill the purpose stated in Section 2.2 above– Authority to Collect.

Biographical/general information

☒ Name	☒ Nationality	☒ Country of Birth
☒ Age	☒ Citizenship	☐ Immigration Status
☒ Date of birth	☒ Ethnicity	☒ Alias (including nickname)
☒ Home physical/postal mailing address	☒ Gender	☒ City or County of Birth
☒ Zip Code	☐ Race	☐ Military Service Information
☒ Personal home phone, cell phone, or fax number	☒ Personal e-mail address	☐ Other (please describe): _____
☒ Country or city of residence	☐ Other (please describe):	☐ Other (please describe):

Other information

☐ Resume or curriculum vitae
☐ Cubical or office number
☐ Veteran's preference
☐ Religion/Religious Preference
☐ Education Information [please describe]
☒ Spouse Information
☒ Professional/personal references or other information about an individual's friends, associates or acquaintances.
☒ Contact lists and directories (known to contain at least some personal information).
☐ Retirement eligibility information
☐ Sexual Orientation
☐ Marital Status
☒ Information about other relatives.
☒ Group/Organization Membership
☒ Information about children
☐ Other (please describe):
☐ Other (please describe):
☐ Other (please describe):
☐ Other (please describe):

Identifying numbers assigned to individuals

☒ Full Social Security number
☐ Personal device identifiers or serial numbers
☒ Vehicle Identification Number
☐ Truncated Social Security Number (e.g., last 4 digits)
☐ Internet Protocol (IP) Address
☒ Driver's License Number
☐ Employee Identification Number
☒ Personal Bank Account Number
☐ License Plate Number
☒ Taxpayer Identification Number
☐ Health Plan Beneficiary Number
☒ Professional License Number
☒ File/Case ID Number
☐ Credit Card Number
☐ Other (please describe):
☒ Alien Registration Number
☐ Patient ID Number
☐ Other (please describe):
☒ Passport Number and information (nationality, date and place of issuance, and expiration date)
☐ Other (please describe):
☐ Other (please describe):

Specific Information/File Types

☒ Taxpayer Information/Tax Return Information
☒ Law Enforcement Information
☐ Security Clearance/Background Check Information
☒ Civil/Criminal History Information/Police Records (obtained from government source)
☐ Civil/Criminal History Information/Police Records (obtained from commercial source)
☐ Credit History Information (government source)
☐ Protected Information (as defined in Treasury Directive 25-10)
☐ Credit History Information (commercial source)
☐ Bank Secrecy Act Information
☐ Information provided under a confidentiality agreement
☐ Case files
☐ Personnel Files
☐ Business Financial Information (including loan information)
☐ Personal Financial Information (e.g., loan information)
☐ Information subject to the terms of an international or other agreement
☒ Passport information (state which passport data elements are collected if not all)
☐ Other (please describe): _____
☐ Other (please describe): _____

Audit Log and Security Monitoring Information

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

☒ Internet Protocol (IP) Address	☐ Video of individuals derived from security cameras	☐ Commercially obtained internet navigation/purchasing habits of individuals
☐ Global Positioning System (GPS)/Location Data	☐ Secure Digital (SD) Card or Other Data stored on a card or other technology	☐ Device settings or preferences (e.g., security level, sharing options, ringtones).
☐ Network communications data	☐ Cell tower records (e.g., logs. user location, time etc.)	☐ Other (please describe): _____

Medical/Emergency Information Regarding Individuals

☐ Medical/Health Information	☐ Worker's Compensation Act Information	☐ Emergency Contact Information (e.g., a third party to contact in case of emergency
☐ Mental Health Information	☐ Information regarding a disability	☐ Patient ID Number
☐ Sick leave information	☐ Request for an accommodation under the Americans with Disabilities Act	
☐ Other_____		

Biometrics/Distinguishing Features/Characteristics of Individuals

☒ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) Identify which are collected: _____	☒ Signatures	☐ Palm prints
☐ Fingerprints	☒ Photos/Video (identify which: _____)	☐ Voice audio recording
☐ Other (please describe): _____	☐ Other (please describe): _____	☐ Other (please describe): _____

Identifying numbers for sole proprietors (including business information).

☐ Sole proprietor business credit card number	☒ Business Phone or Fax Number	☒ Business Physical/Postal Mailing Address
☐ Sole proprietor business professional license number	☐ Sole proprietor business file case number	☒ Sole proprietor business taxpayer identification number
☐ Sole proprietor business license plate number	☐ Sole proprietor business vehicle identification number	☒ Sole proprietor business bank account number
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe):

3.3 Sources from which PII is obtained

Collection/Acquisition from Individuals

1. Members of the Public

☒ Members of the Public (i.e., including individuals who are current federal employees who are providing the information in their "personal" capacity (unrelated to federal work/employment). All of the following are members of the public. Please check relevant boxes (based on the context of collection and use in this system) for members of the public whose information is maintained in the system (only check if relevant to the purpose for collecting and using the information):

☒ Members of the general public (current association with the federal government, if any, is irrelevant to the collection and use of the information by the system or project). *Information regarding individuals (US citizens and LPRs) and foreign nationals is maintained and used in OCTS system.*

☐ Retired federal employees. Discuss **here** how/why PII is collected from this source.

☐ Former Treasury employees. Discuss **here** how/why PII is collected from this source.

☐ Federal contractors, grantees, interns, detailees etc. Discuss **here** how/why PII is collected from this source.

☐ Federal job applicants. Discuss **here** how/why PII is collected from this source

☒ Other: [Explain ***here***]. *SDN data is derived from several sources, including open source/internet research, news articles, federal intelligence data, and federal law enforcement data.*

2. Current Federal Employees, Interns, and Detailees

☐ Current Federal employees providing information in their capacity as federal employees (for example, PII collected using OPM or Treasury forms related to employment with the federal government) ☐ Interns. .

☐ Detailees. Discuss **here** how/why PII is collected from this source.

☐ Other employment-related positions. [name the position **here** and discuss how/why PII is collected from this source.].

3. Treasury Bureaus (including Departmental Offices)

☐ Other Treasury Bureaus: [name the bureau(s) **here** and identify the bureau/office information system from which the PII originated) and how/why PII is collected from this source].

4. Other Federal Agencies

☒ Other federal agencies: *SDN data are collected from Federal Law enforcement agencies and Federal intelligence agencies related to foreign asset control (unclassified).*

5. State and Local Agencies

☐ State and local agencies: [name the State and local agencies **here** and explain how/why PII is collected from this source].

6. Private Sector

☒ Private sector organizations (for example, banks and financial organizations, data brokers or other commercial sources): *All financial organizations are legally required to report blocked and rejected transactions.*

7. Other Sources

☒ Other sources not covered above (for example, foreign governments).
Data provided per international agreements and alliances with foreign governments.

Section 3.3: Privacy and/or civil liberties risks related to collection

When Federal agencies request 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 [the individual], if any, of not providing all or any part of the requested information." 5 U.S.C § 522a(e)(3). This is commonly called a Privacy Act Statement. The OMB Guidelines also note that subsection (e)(3) is applicable to both written and oral (i.e., interview) solicitations of personal information. Therefore, even if a federal employee or contractor has a fixed list of questions that they orally ask the individual in order to collect their information, this requirement applies.

Section 3.3(a) Collection Directly from the Individual to whom the PII pertains

1. ☐ None of the PII in the system was collected directly from an individual to whom it pertains. . *[Explain **here** if the third-party/agency from which you obtained the PII actually collected the*

PII directly from the individuals about whom it pertains. Be prepared to discuss below how you ensure the information received from the third-party is still accurate, complete and timely for the purposes for which you will use it)].

2. ☒ Some of the information in this system was collected directly from an individual to whom it pertains.

Section 3.3(b) Privacy Act Statements

1. ☐ None of the PII in the system was collected directly from the individuals to whom it pertains. Therefore, a Privacy Act Statement is not required. ***here***
2. ☒ Some of the PII in the system was collected directly from the individual to whom it pertains. Therefore, a Privacy Act Statement was posted at the point where the PII was collected directly from the individual. That Privacy Act Statement was provided to the individual ☐ on the form in which the PII was collected ☐ on a separate sheet of paper that the individual could retain; or ☐ in an audio recording or verbally at the point where the information was collected (e.g., on the phone) or ☒ *Electronically prior to submission on the Licensing Site*.
3. The Privacy Act Statement contained the following:
    a. ☒ The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
    b. ☒ Whether disclosure of such information is mandatory or voluntary.
    c. ☒ The principal purpose or purposes for which the information is intended to be used.
    d. ☒ The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
    e. ☒ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

Section 3.3(c) Use of Full Social Security Numbers

Treasury is committed to eliminating unnecessary collection, use, and display of full Social Security numbers ("SSN") and redacting, truncating, and anonymizing SSNs in systems and documents to limit their accessibility to individuals who do not have a need to access the full SSN in order to perform their official duties. Moreover, the Privacy Act provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *Id.* at § 7(a)(2)(A)-(B).

Section 3.3(d) Justification for collection and use of the full Social Security Numbers

1. ☐ N/A No full SSNs are maintained in the system or by the project. [*Explain **here** if any portion of the SSN short of the full 9 digits is used in the system; if the full SSN is located anywhere in the system (even if it is redacted, truncated or anonymized when viewed by users, please check number 2 below)*].
2. ☒ Full SSNs are maintained in the system or by the project and the following approved Treasury uses of SSNs apply:

    ☐ security background investigations;

    ☐ interfaces with external entities that require the SSN;

☐ a legal/statutory basis (e.g. where collection is expressly required by statute);

☐ when there is no reasonable, alternative means for meeting business requirements;

☐ statistical and other research purposes;

☐ delivery of government benefits, privileges, and services;

☒ for law enforcement and intelligence purposes (to distinguish between individuals with the same or similar names);

☐ aging systems with technological limitations combined with funding limitations render impracticable system modifications or replacements to add privacy risk reduction tools (partial/truncated/redacted or masked SSNs); and

☒ as a unique identifier for identity verification purposes.

Section 3.3(e) Controls implemented to limit access to and or improper disclosure of full Social Security Numbers

1. ☐ Full SSNs are ***not*** maintained in the system or by the project.
2. ☒ Full SSNs ***are*** maintained in the system or by the project and the following controls are put in place to reduce the risk that the SSN will be seen or used by someone who does not have a need to use the SSN in order to perform their official duties (*check **ALL** that apply*):
    a. ☐ The entire SSN data field is capable of suppression (i.e., being turned off) and the data field is suppressed when the SSN is not required for particular system users to perform their official duties.
    b. ☐ do not require the SSN to perform their official duties.☐ Within the system, an alternative number (e.g., an Employee ID) is displayed to all system users who do not require the SSN to perform their official duties. The SSN is only linked to the alternative number within the system and when reporting outside the system (to an agency that requires the full SSN). The SSN is not visible to system users (other than administrators).
    d. ☐ The SSN is truncated (i.e., shortened to the last 4 digits of the SSN) when displayed to all system users for whom the last four digits (but not the full) SSN are necessary to perform their official duties.
    e. ☐ Full or truncated SSNs are only downloaded to spreadsheets or other documents for sharing within the bureau or agency when disclosed to staff whose official duties require access to the full or truncated SSNs for the particular individuals to whom they pertain. No SSNs (full or truncated) are included in spreadsheets or documents unless required by each recipient to whom it is disclosed in order to perform their official duties (e.g., all recipients have a need to see the SSN for each employee in the spreadsheet).
    f. ☒ Other: [*The SSNs for the US citizens designated and placed on the SDN list are publicly available. Information provided to OFAC by the financial institutions under 31 CFR Chapter V includes SSN.]*.

Section 3.3(f) Denial of rights, benefits, or privileges for refusing to disclose Social Security Number

1. ☐ No SSNs are maintained in the system or by the project.

2. ☒ Full SSNs are collected, but no individual will be denied any right, benefit, or privilege provided by law if the individual refuses to disclose their SSN for use in the system or project. *The individuals being designated are not providing their SSN. It is obtained from other sources to identify the individual associated with the SSN. OFAC does not actively collect the SSN. Information reported to OFAC by the financial institutions includes SSN. 31 CFR chapter V requires financial institutions to provide a description of any transaction associated with the blocking, including: The type of transaction; any persons, including financial institutions, participating in the transaction and their respective locations (e.g., if relevant, customers, beneficiaries, originators, letter of credit applicants, and their banks; intermediary banks; correspondent banks; issuing banks; and advising or confirming banks); and any reference numbers, dates, or other information necessary to identify the transaction. The SSN is only used in specific cases as an identifier for US citizens and/or LPRs being designated.*
3. ☐ Full SSNs are collected, and the individual ***will*** be denied the following right, benefit, or privilege provided by law if they refuse to disclose their SSN: *[please identify **here** the right, benefit, or privilege if the individual will be denied if they choose not to provide their SSN]*. Denial of this right, benefit or privilege does not violate the law because: *[choose one of the two boxes below]:*
   a. ☐ SSN disclosure is required by the following Federal statute or Executive Order; **OR**
   b. ☐ The SSN is disclosed to a Federal, state, or local agency that maintains a system of records that was in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

Section 3.3(g) Records describing how individuals exercise First Amendment rights

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." 5 U.S.C. § 552a(e)(7).

Please check the statement below that applies to your system or project and provide the additional information requested. Please read all possible responses before selecting an answer. ☒ N/A. The system or project does ***not*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment.

2. ☐ The system or project ***does*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment. *If you checked this box, please check the box below that explains Treasury's authorization for collecting this information:*

   a. ☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance. The individual about whom the information was collected or maintained expressly authorized its collection by *[explain **here** how the individual expressly authorizes collection] (for example, individuals may expressly authorize collection by requesting in writing that Treasury share information with a third party, e.g., their Congressman];*
   b. ☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity because [*generally discuss **here** the nature and purpose of the information collected and the law enforcement activity*];

c. ☐ The following statute expressly authorizes its collection: [*provide **here** the name of **and** citation to the statute **and** the language from that statute that expressly authorizes collection*] [*your response MUST contain all three if you use a statute as the basis for the collection*].

Section 4: Maintenance, use, and sharing of the information

Section 4.1: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared when it is used to make determinations about individuals

The Privacy Act and Treasury policy require that Treasury bureaus and offices take additional care when collecting and maintaining information about individuals when it will be used to make determinations about those individuals (e.g., whether they will receive a federal benefit). This includes collecting information directly from the individual where practicable and ensuring that the information is accurate, relevant, timely and complete to assure fairness to the individual when making a determination about them. This section addresses the controls/protections put in place to address these issues.

The Privacy Act requires that Federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C § 552a(e)(5). If a particular system of records meets certain requirements (including the NPRM process defined in Section 3.1 above), an agency may exempt the system of records (or a portion of the records) from this requirement. Exemptions may be found at the bottom of the relevant SORN next to the heading: "*Exemptions Claimed for this System.*"

Section 4.1(a). Exemption from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act

1. ☒ ***None*** of the information maintained in the system or by the project that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act.
2. ☐ All ☐ Some of the PII maintained in the system or by the project is part of a system of records and ***is*** exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act. The exemption claimed for these records is appropriate because *[please see Appendix B which contains sample justifications for this exemption and provide the appropriate bases **here** [more than one bases may apply]*.
3. ☐ The PII maintained in the system or by the project is ***not***: (a) part of a system of records as defined in section (e)(5) of the Privacy Act; or (b) used to make adverse determinations about individuals (defined in the Privacy Act as U.S. Citizens and legal permanent residents). Instead, the information is used to [*describe how the information is used and why this use does not involve adverse determinations*]. *hat you read the rest of the options before checking this box*☐ ***None*** of the information maintained in the system or by the project is part of a system of records as defined in section (e)(5) of the Privacy Act, but the information in the system ***is*** used to make adverse determinations about individuals (defined in the Privacy Act as U.S. Citizens and legal permanent residents). Despite the fact that the Privacy Act does not apply, the following protections are in place to ensure fairness to the individual: *explain **here*** .

Section 4.1(b) Protections in place despite exemption from the accuracy, relevance, timeliness, and completeness requirements

1. ☒ ***None*** of the information maintained in the system or by the project that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act.
2. ☐ For all information maintained in the system or by the project that is part of a system of records that is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act, the following efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible without interfering with the (*check one*) ☐ law enforcement ☐ intelligence ☐ other [*describe **here***] mission requirements for which the system or project was created [*choose **ALL** that apply*]:
    a. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals.
    b. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals without additional research and investigation to ensure accuracy, relevance, timeliness, and completeness.
    c. ☐ Individuals and organizations to whom PII from the system or project is disclosed (as authorized by the Privacy Act) determine its accuracy, relevance, timeliness, and completeness in a manner reasonable for their purposes before they use it to make adverse determinations about individuals.
    d. ☐ Individuals about whom adverse determinations are made using PII from this system or project are given an opportunity to explain or modify their information (*check one*) ☐ before ☐ after the adverse determination is made. During this process, individuals are allowed to: [*discuss **here***
    e. ☐ Other: (*please describe*):
3. ☐ No additional efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible because it would interfere with mission requirements.

Section 4.1(c) Collecting information directly from the individual when using it to make adverse determinations about them

Section 552a(e)(2) of the Privacy Act requires that Federal agencies that maintain records in a system of records are required to collect information to the greatest extent practicable directly from the individual when the information about them may result in adverse determinations about their rights, benefits, and privileges under Federal programs. Agencies may exempt a system of records from this requirement under certain circumstances and if certain conditions are met.

1. ☐ The records maintained by this system or project are **not** used to make any adverse determinations about individuals.
2. ☒ The records maintained by this system or project **are** used to make adverse determinations about individuals ***and*** *[check all that apply]:*
    a. ☐ These records ***were*** exempted from the Privacy Act provision that requires collection directly from the subject individual to the greatest extent practicable. Exemption of these records is proper because *[explain **here** why the records were exempted; sample responses are provided in Appendix B of this template]*.
    b. ☒ These records were ***not*** exempted from the requirement to collect information directly from the individual to the greatest extent practicable ***and*** [*check the relevant box below and provide the information requested*].
        i. ☐ ***All*** records used to make an adverse determination are collected directly from the individual about whom the decision is made.
        ii. ☒ A ***combination*** of records collected from third parties ***and*** directly from the individual about whom the determination is made are used to make the determination because *ABaRRS HV data is provided to OFAC primarily by*

financial institutions reporting blocked or rejected transactions per their legal obligations. Although most of these reports come from financial institutions, every American citizen and organization has an obligation to report blocked or rejected transactions. Pursuant to 31 CFR § 501.604, "any U.S. person (or person subject to U.S. jurisdiction), including a financial institution, that rejects a transaction that is not blocked under the provisions of this chapter, but where processing or engaging in the transaction would nonetheless violate a provision contained in this chapter, shall submit a report to OFAC."

OASIS data is received from mail correspondence, including license applications sent from the individuals or businesses/corporations to OFAC. Additionally, OASIS contains investigative research, penalty and payment information and other supplemental data that might be submitted to OFAC by the public. Case data may also be derived from the news media or Federal law enforcement agencies.

SDN data is derived from several sources, including open source/internet research, news articles, Federal intelligence data, Federal law enforcement data and data provided per international agreements and alliances with foreign governments.].

iii. ☒ ***Some*** of the records used to make adverse determinations are not collected directly from the individual about whom determinations are made because seeking the information directly from the individual might *[select **ALL** that apply]:*

☒ alert the individual to the fact that their conduct is being observed or investigated;

☒ cause the individual to alter or modify their activities to avoid detection;

☒ create risks to witnesses or other third parties if the individual is alerted to the fact that their conduct is being observed or investigated;

☐ Other: *(please describe **here**).*

Section 4.1(d) Additional controls designed to ensure accuracy, completeness, timeliness and fairness to individuals in making adverse determinations

1. **Administrative Controls**. Individuals about whom information is collected are given the following opportunities to amend/correct/update their information to ensure it is accurate, timely and complete to the extent reasonably necessary to assure fairness when it is used to make a determination about them

a. ☐ The PII collected for use in the system or project is NOT used to make adverse determinations about an individual's rights, benefits, and privileges under federal programs.

b. ☒ The records maintained in the system or by the project are used to make adverse determinations and (*select one*) ☒ are exempt from the access provisions in the Privacy Act, 5 U.S.C. 552a(d). *Records in this system that are related to enforcement, designation, blocking, and other investigations are exempt from the provisions of the Privacy Act as permitted by 5 U.S.C. 552a(k)(2). Exempt records may not be disclosed for purposes of determining if the system contains a record pertaining to a particular individual, inspecting records, or contesting the content of records. Although the investigative records that underlie the SDN List may not be accessed for purposes of inspection or to contest of content of records, the SDN List, which is produced from some of the investigative records in the system, is made public. Entities and individuals*

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

c. ☒ Treasury has published regulations in place describing how individuals may seek access to and amendment of their records under the Privacy Act. *The Treasury/bureaus FOIA and Privacy Act disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C.*

d. ☐ Individuals who provide their information directly to Treasury for use in the system or by the project are provided notice of the adverse determination and an opportunity to amend/correct/ update their information *[choose one]* ☐ before ☐ after it is used to make a final, adverse determination about them. This is accomplished by: [*describe **here** how this process works and the protections in place, including redress/appeals processes; if notice is provided **after** an adverse determination is made, explain **here** why notice could not be provided **before** a determination was made, and the protections in place*].

e. ☐ Individuals who provide their information directly to Treasury for use in the system or by the project are expressly told at the point where the information is collected that they need to keep their information accurate, current and complete because it could be used to make adverse determinations about them. This is accomplished by: [*describe **here** how/where/when individuals are told they need to keep their information updated before it is used to make adverse decisions about them; include the exact language provided to the individuals*].

f. ☐ All manual PII data entry by federal employees/contractors is verified by a supervisor or other data entry personnel before it is uploaded to the system (e.g., PII entered into the system from paper records is double-checked by someone else before it's uploaded to the system). This is accomplished by: [*describe **here** how this process works*].

g. ☐ Other: [*please describe **here***].

2. Technical controls. The system or project also includes additional technical controls to ensure that PII is maintained with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual when it is used to make a determination about them. The following additional protections are relevant to this system or project ☐ No additional technical controls are available to ensure accuracy, relevance, timeliness and completeness.

b. ☐ Automated data feeds are used to refresh/update the information in the system (where the system is reliant on updates from another system). These automated data feeds occur: [*state **here** the frequency of updates*] and [*state **here** what happens when the data is updated and why the system is reliant on another system for its data*].

c. ☐ Technical and/or administrative controls put are in place to ensure that when information about an individual is acquired from multiple sources for maintenance in a single file about a particular individual, it all relates to the same individual. This is accomplished by: [*describe **here** the method or process used to ensure that information merged about an individual from multiple sources for inclusion in a single file, all relates to the same person*].

d. ☐ Address verification and correction software (software that validates, updates and standardizes the postal addresses in a database).

e. ☒ Other: *Overall, all the OCTS component applications use a three tiered architecture of information input validations to control the completeness and accuracy of the information entered. These include database constraints, business object constraints,*

and user interface constraints. Redundancy checks are built into the architecture so that if an input validation is missed at one tier, it can be identified at another tier. These input validation checks include reconciliations, pre-filled fields, and specific data input and pre-defined acceptable value requirements for fields. OFAC developed the OCTS applications to provide a message to the end-user notifying them of the input error. When working in concert together, these information input validations have been designed to maintain data integrity within the information system and prevent erroneous information from being entered (including malicious commands).

External OCTS users are only allowed to upload information via web-based access to the ABaRRS HV and Licensing applications. For ABaRRS HV, this information is limited to xml files containing blocked or rejected financial transactions, payment/transfer instructions and relevant documentation. Access is limited to individuals that have successfully registered with Treasury's approved identify provider that makes use of multifactor authentication and identify proofing. The public facing Licensing application allows external OCTS users to upload PDF documents related to their application or blocked transactions. This input is initially processed by a publicly accessible web server before being transmitted to the backend database. Before the data is transmitted to the backend database server, a batch process is performed to format correctly all inputted data for delivery. Once the data is correctly formatted and determined to be complete, it is transferred securely to the backend OCTS database server, OCTS internal users further process and verify the data for completeness. A two-way secure shell connection securely transmits information between the OCTS web server and the OCTS backend database server.

Section 4.2 Data-Mining

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

Section 4.2(a) Is the PII maintained in the system used to conduct data-mining?

1. ☒ The information maintained in this system or by this project ***is not*** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act. Therefore, no privacy or civil liberties issues were identified in responding to this question.
2. ☐ The information maintained in this system or by this project ***is*** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act. This system is included in Treasury's annual report to Congress which can be found on the external Treasury privacy website. [NEED LINK].
3. ☐ The information maintained in this system or by this project ***is*** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act, but this system is not included in Treasury's annual report to Congress which can be found on the external Treasury privacy website. This system will be added to the next Treasury Data-mining report to Congress.

Section 4.3 Computer Matching

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

to the CMPPA, 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 (the agency providing the records) and recipient agency (the agency that receives and uses the records to make determinations). The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

Section 4.3(a) Records in the system used in a computer matching program *Please check the statement below that applies to your system or project and provide the additional information requested for each box you checked. Please read all possible responses before selecting an answer*

1. ☐ The PII maintained in the system or by the project ***is not*** part of a Privacy Act system of records.
2. ☒ The information maintained in the system or by the project ***is*** part of a Privacy Act system of records, but ***is not*** used as part of a matching program.
3. ☐ The information maintained in the system or by the project ***is*** part of a Privacy Act system of records and ***is*** used as part of a matching program. [*Explain **here** whether a Matching Agreement was executed and published as required by the CMPPA/Privacy Act; if no Matching Agreement was executed, please explain here why*].

Section 4.3(b) Is there a matching agreement?

1. ☒ N/A
2. ☐ There is a matching agreement in place that contains the information required by Section (o) of the Privacy Act.

☐ There is a matching agreement in place, but it does not contain all of the information required by Section (o) of the Privacy Act. The following actions are underway to amend the agreement to ensure that it is compliant:

Section 4.3(c) What procedures are followed before adverse action is taken against an individual who is the subject of a matching agreement search?

*Please check **ALL** statements below that apply to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.*

1. ☒ N/A
2. ☐ The bureau or office that owns the system or project conducted an assessment regarding the accuracy of the records that are used in the matching program and the following additional protections were put in place:
   a. ☐ The results of that assessment were independently verified by [*explain how and by whom accuracy is independently verified; include the general activities involved in the verification process*].
   b. ☐ Before any information subject to the matching agreement is used to suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to an individual:
      i. ☐ The individual receives notice and an opportunity to contest the findings; **OR**

ii. ☐ The Data Integrity Board approves the proposed action with respect to the financial assistance or payment in accordance with Section (p) of the Privacy Act before taking adverse action against the individual.

3. ☐ No assessment was made regarding the accuracy of the records that are used in the matching program.

Section 4.4: Information sharing with external (i.e., outside Treasury) organizations and individuals

Section 4.4(a) PII shared with/disclosed to agencies, organizations or individuals outside Treasury

1. ☐ PII maintained in the system or by the project is ***not*** shared with agencies, organizations, or individuals external to Treasury.
2. ☐ PII maintained in the system or by the project ***is*** shared with the following agencies, organizations, or individuals external to Treasury: [*For each recipient, provide the following: (1) name of organization/type of individual; (2) the PII shared; (3) the purpose of the sharing; (4) identify any statutes that limit use or sharing of the information; (5) identity any applicable MOU*].
3. ☒ All external disclosures ***are*** authorized by the Privacy Act (including routine uses in the applicable SORN).

Section 4.4(b) Accounting of Disclosures

An accounting of disclosures is a log of all external (outside Treasury) disclosures of records made from a system of records that has ***not*** been exempted from this accounting requirement. This log must either be maintained regularly or be capable of assembly in a reasonable amount of time after an individual makes a request. Certain system of records may be exempted from releasing an accounting of disclosures (e.g., in law enforcement investigations).

Check toward the bottom of the SORN to see whether an exemption was claimed from 5 U.S.C. 552a(c). The NPRM and/or Final Rule for the system of records will explain why that exemption is appropriate.

Section 4.4(c) Making the Accounting of Disclosures Available

☐ The records are not maintained in a system of records subject to the Privacy Act so an accounting is ***not*** required.

2. ☐ No external disclosures are made from the system.
3. ☒ Portions of the Privacy Act system of records maintained in the system or by the project ***is*** exempt from the requirement to make the accounting available to the individual named in the record. Exemption from this requirement was claimed because: *Records in this system that are related to enforcement, designation, blocking, and other investigations are exempt from the provisions of the Privacy Act as permitted by 5 U.S.C. 552a(k)(2). Exempt records may not be disclosed for purposes of determining if the system contains a record pertaining to a particular individual, inspecting records, or contesting the content of records. Although the investigative records that underlie the SDN List may not be accessed for purposes of inspection or for contest of content of records, the SDN List, which is produced from some of the investigative records in the system, is made public. Persons (entities and individuals) on this public list who wish to request the removal of their name from this list may submit a de-listing petition according to the provisions of 31 CFR*

501.807. This request must be made in writing and addressed to the Director, Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, NW. - Annex, Washington, DC 20220].

4. ☒ Portions of the Privacy Act system of records maintained in the system or by the project are ***not*** exempt from the requirement to make the accounting available to the individual named in the record and a log is maintained regularly. The log is maintained for at least five years and includes 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. *For records in this system that are unrelated to enforcement, designation, blocking, and other investigations, individuals wishing to gain access to records maintained in the system under their name or personal identifier must submit a written request containing the following elements: (1) Identify the record system; (2) identify the category and type of record sought; and (3) provide at least two items of secondary identification (date of birth, employee identification number, dates of employment, or similar information). Address inquiries to Assistant Director, Disclosure Services, Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue NW., Washington, DC 20220. The request must be made in accordance with 5 U.S.C. 552a and 31 CFR 1.2. See also 31 CFR part 1, subpart C, appendix A, Paragraph 8.*
5. ☐ The Privacy Act system of records maintained in the system or by the project is ***not*** exempt from the requirement to make the accounting available to the individual named in the record and a log is ***not*** maintained regularly, but is capable of being constructed in a reasonable amount of time upon request. The information necessary to reconstruct the log (i.e., date, nature, and purpose of each disclosure) is maintained for at least five years.

Section 4.4(d) Obtaining Consent Prior to New Disclosures Not Authorized by the Privacy Act

Records in a system of records subject to the Privacy Act may not be disclosed by "any means of communication to any person or to another agency" without the prior written request or consent of the individuals to whom the records pertain. 5 U.S.C. Sec. 552a(b). However, the Act also sets forth twelve exceptions to this general restriction. These 12 exceptions may be viewed at: https://www.justice.gov/usam/eousa-resource-manual-139-routine-uses-and-exemptions
Unless one of these 12 exceptions applies, the individual to whom a record pertains must provide their consent, where feasible and appropriate, before their records may be disclosed to anyone who is not listed in one of the 12 exceptions. One of these 12 exceptions also allows agencies to include in a notice published in the Federal Register, a list of routine uses. Routines uses are disclosures outside the agency that are compatible with the purpose for which the records were collected.

Section 4.4(e) Obtaining Prior Written Consent

1. ☒ The records maintained in the system of records are only shared in a manner consistent with one of the 12 exceptions in the Privacy Act, including the routine uses published in the Federal Register.
2. ☒ If a situation arises where disclosure (written, oral, electronic, or mechanical) must be made to anyone outside of Treasury who is not listed in one of the 12 exceptions in the Privacy Act (including the published routine uses), the individual's prior written consent will be obtained where feasible and appropriate. *This applies only to records in the system that are unrelated to enforcement, designation, blocking, and other investigations*

Section 5: 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 5.1: 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 also requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

Section 5.1(a)

1. ☒ The system or project maintains information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government).
2. ☒ The project or system involves a new collection of information in identifiable form for 10 or more persons from outside the federal government.
3. ☒ The project or system completed an Information Collection Request ("ICR") and received OMB approval. *OMB No. 1505-0170* (*SDN does not require ICR)*
4. ☐ The project or system did not complete an Information Collection Request ("ICR") and receive OMB approval because.

Section 5.2: 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 National Archives and Records Administration (NARA) for permanent retention upon expiration of this period. If the system has an applicable SORN(s), check the "Policies and Practices for Retention and Disposal of Records" section.

Section 5.2(a)

1. ☒ The records used in the system or by the project are covered by a NARA's General Records Schedule (GRS). *The OFAC schedule governing these documents is N1-056-02-004.*
2. ☐ The records used in the system or by the project are covered by a NARA approved Treasury bureau Specific Records Schedule (SRS). The SRS *[please provide **here** the specific schedule name and identifying number]*.
3. ☐ On [*please state the date on which NARA approval was sought*] the system owner sought approval from NARA for an SRS and is awaiting a response from NARA. *[State **here** the retention periods you proposed to NARA*].

Section 5.3: E-Government Act/NIST Compliance

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

Section 5.3(a)

1. ☒ The system is a federal information system subject to FISMA requirements.
2. ☒The system last completed an SA&A and received an ATO on: 30 June, 2019
3. ☐This is a new system has not yet been authorized to operate. The expected to date for receiving ATO is *[please state **here** the expected date on which you expect authorization will be granted]*.
4. ☐The system or project maintains access controls to ensure that access to PII maintained is limited to individuals who have a need to know the information in order to perform their official Treasury duties.
5. ☒ All Treasury/bureau security requirements are met when disclosing and transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury system or project to internal or external parties.
6. ☒ This system or project maintains an audit log of system users to ensure they do not violate the system and/or Treasury/bureau rules of behavior.
7. ☐ This system or project has the capability to identify, locate, and monitor individuals or groups of people other than the monitoring of system users to ensure that they do not violate the system's rules of behavior. *[If checked, please describe this capability **here**, including safeguards put in place to ensure the protection of privacy and civil liberties.]*

Section 5.4: Section 508 of the Rehabilitation Act of 1973

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

Section 5.4(a)

1. ☐ The project or system will ***not*** 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).
2. ☒ The project or system ***will*** 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
3. ☒ The system or project complies 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. *The public facing applications including modernized Public Licensing have been reviewed and tested for adherence to the 508 compliance guidelines.*
4. ☐ The system or project is not in compliance with all Section 508 requirements. The following actions are in progress to ensure compliance:

Responsible Officials

Approval Signature

_____

Timothy H. Skinner
Bureau Privacy and Civil Liberties Officer
Departmental Offices & Records