Privacy and Civil Liberties Impact Assessment

for the

Treasury Office of Foreign Assets Control (OFAC) Systems (TOS)

March 25, 2026

Contact Point

Dennis Blount
Office of Foreign Assets Control

Reviewing Official

Ryan Law
Deputy Assistant Secretary
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; and (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy.

Section 2: Artificial Intelligence (AI)

The Department of the Treasury is leveraging AI to better serve the public across a wide array of use cases and benefits delivery. This section describes how this information system will utilize AI.

1. The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.
2. The term "AI model" means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.
3. The term "AI red-teaming" means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. Artificial Intelligence red-teaming is most often performed by dedicated "red teams" that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.
4. The term "AI system" means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

5. The term "crime forecasting" means the use of analytical techniques to attempt to predict future crimes or crime-related information. It can include machine-generated predictions that use algorithms to analyze large volumes of data, as well as other forecasts that are generated without machines and based on statistics, such as historical crime statistics.

The Department of the Treasury is leveraging AI to better serve the public across a wide array of use cases and benefits delivery. Treasury is also establishing strong guardrails to ensure its use of AI keeps individual safe and doesn't violate their rights. [Check all that apply]:

This PCLIA is being conducted on:

1- ☐ an information system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments using machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.
2- ☐ an information system that maintains a component that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.
3- ☐ an information system that will be used, in part, as a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI.
4- ☐ an information system that includes software, hardware, application, tool, or utility that operates in whole or in part using AI.
5- ☐ an information system that uses analytical techniques to attempt to predict future crimes or crime-related information. It can include machine-generated predictions that use algorithms to analyze large volumes of data, as well as other forecasts that are generated without machines and based on statistics, such as historical crime statistics(Please stop here if you check any of the 5 boxes above and use the AI Systems PCLIA template to continue.
6- ☒ None of the above. (Please continue with this template if checked).

3: System Overview

3.1: System/Project Description and Purpose and Purpose

The Department of the Treasury's Office of Foreign Assets Control (OFAC) owns the system and associated technologies (hereinafter referred to for purposes of these instructions as the "system") is conducting this PCLIA for the Treasury OFAC System (TOS). The system is updating a previous PCLIA for this system that was approved on January 15, 2026.

This PCLIA is being updated to reflect a recent development. OFAC and Treasury's Financial Crimes Enforcement Network (FinCEN) are jointly issuing new regulations to implement provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act). This regulation will, among other things, treat permitted payment stablecoin

issuers (PPSIs) as financial institutions for purposes of the Bank Secrecy Act and establish specific sanctions compliance program (SCP) obligations for PPSIs. The new SCP for PPSIs includes an information collection requirement. This new collection pertains to testing and auditing recordkeeping requirements. PPSIs will be required to maintain, and provide upon request to OFAC, records of the testing and audit results and enhancements of their sanctions compliance programs, which would normally include the company's name, address, telephone number, point of contact, and copies of the testing and auditing reports. Information collected under this requirement will be stored in the Office of Foreign Assets Control's Administrative System for Investigation and Sanctions (OASIS), OFAC's official system of record for licensing, compliance, and enforcement activities.
This revised assessment aligns the TOS PCLIA with the most current standards while addressing the expanded system scope.

The main purpose of the Department of the Treasury's Office of Foreign Assets Control is to administer and enforce 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 several sanctions lists that include individuals, entities (organizations, companies, etc.), aircraft, and vessels along with identifying information for each. The lists include, among other things, terrorists, narcotics traffickers, individuals acting for or on behalf of targeted countries, as well as companies owned or controlled by the designated individuals. The legal criteria for adding a target to one of OFAC's sanctions lists varies depending on the sanctions program and the underlying legal authorities. OFAC currently administers over 30 sanctions programs, each with a unique set of legal criteria for adding a target to one of OFAC's sanctions lists.

At a high level, a group within OFAC identifies targets under one or more of the various sanctions programs, researches the basis for designation/identification as well as publicly releasable identifiers and puts together the evidentiary packages needed. The package goes through a robust legal review and vetting process. Many of the targets are published on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) and are referred to as "Specially Designated Nationals" or "SDNs." All property and interests in property of these persons that come within the possession of U.S. persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. 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.

The TOS underpins OFAC's mission by providing the core technology platforms, services, and websites that enable the identification, investigation, designation, and publication of sanctioned parties. The TOS supports the full lifecycle of sanctions administration from the intake and management of evidentiary packages to the legal review workflow and final approval processes. TOS also hosts and maintains the public facing websites that disseminate sanctions information, enabling government agencies, financial institutions, and private entities to comply with U.S.

sanctions regulations. Through these capabilities, TOS operationalizes sanctions policy and enforces compliance across a global audience.

TOS hosts both internal and public-facing applications, including the OFAC Sanctions List Search tool, OFAC Sanctions List Service, OFAC Public Licensing, OFAC Reporting System (ORS), OFAC Disclosure Portal, OFAC Sanctions Reconsideration Portal, and the OASIS. These tools collectively support transparency, compliance, reporting, and case management, while broadening access to OFAC services. The system directly supports Treasury's Primary Mission Essential Function (PMEF #2: Impose Trade Sanctions) and multiple Mission Essential Functions (MEFs).

TOS is comprised of the applications listed below:

a) Sanctions List Search ("Sanctions Search") (T-CLOUD hosted) <https://sanctionssearch.ofac.treas.gov> – All financial institutions and persons in the U.S. are required to block or reject 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 screening of all OFAC sanctions lists, including the SDN List. Sanctions list data, including SDN data, is derived from several sources, including open source/internet research, news articles, commercial databases, corporate filings, Federal intelligence data, Federal law enforcement data and data provided per international agreements and alliances with foreign governments, among other things. Sanctions list data is unclassified and includes identifying information related to individuals, organizations, companies, vessels, and aircraft designated/identified pursuant to one of OFAC's sanctions programs. Although the vast majority of sanctions list data relates to foreign nationals, a very small portion relates to US citizens, Lawful Permanent Residents (LPRs) and US-based entities or blocked property. The Sanctions Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions 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 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 Search invokes fuzzy logic when the tool is run. The other fields on the tool use character matching logic.

b) The Sanctions List Search tool does not collect any PII from users. It is provided solely as a public service to help individuals and organizations search the OFAC sanctions lists, such as the Specially Designated Nationals (SDN) List. When a user enters a name or term into the search field, the query is processed in real time against the published sanctions data, but the information entered is not stored, logged, or shared by OFAC. The tool functions strictly as a lookup service and does not retain search terms, user details, or any other identifying information. Its purpose is limited to improving public access to the

official sanctions lists.

c) OFAC Reporting System (ORS) (T-CLOUD hosted) <https://ors.ofac.treas.gov> - 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. ORS is one of two TOS component with registered external users. Although all US persons are required to block or reject and then report certain transactions, ORS 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 ORS, 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 foreign nationals, US. citizens and LPRs.

ORS collects PII necessary to process sanctions-related reports submitted to OFAC. For filers, ORS collects basic identifiers such as name, address, job title, phone number, and email address. ORS also collects financial and transactional information, including bank account numbers, payment details, and information about counterparties to reported transactions. In addition, any supporting documentation uploaded through ORS may contain PII. PII collected regarding parties to a transaction typically include a name and some address information. All information collected is transmitted and stored securely, accessible only to authorized OFAC personnel, and handled in accordance with Treasury privacy policies and applicable federal regulations.

ORS collects PII only insofar as it is necessary to record and investigate blocked or rejected transactions reported under U.S. sanctions laws.

d) Public Facing Licensing (T-CLOUD hosted) <https://ofaclicensing.ofac.treas.gov> – Public Facing Licensing is a customized web-based information system that supports OFAC's requirements for receiving applications and issuing licenses to the public. The licenses are 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. License 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; applicants are instructed not to submit an application for a specific license)

- Application for the release of blocked funds, wire transfers at a U.S. financial institution
- 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.
- Application for a specific license or interpretive guidance in all other circumstances ("Transactional")

The Licensing application portals collect PII from individuals and organizations that submit requests to OFAC for licenses, guidance, or related determinations. This may include basic identifiers such as name, date of birth, address, phone number, and email address, as well as organizational information like company name, tax identification number, or employer identification number and includes US Citizens, Lawful Permanent Residents and Foreign nationals. Depending on the type of license request, supporting documentation submitted may also contain PII, such as passport numbers, financial account information, or other personal details relevant to the application. This information is collected only for the purpose of reviewing and processing license requests and is safeguarded in accordance with Treasury privacy and security requirements. OFAC limits access to this information to authorized personnel and protects all submissions using secure connections and encryption.

e) Trade Sanctions Reform and Export Enhancement Act of 2000 (TSRA) (T-CLOUD hosted) <https://tsra.ofac.treas.gov> – OFAC has endeavored to implement the TSRA in a way that is consistent with both the statutory language and the intent of its drafters and in a manner that also provides exporters with an efficient and expedited process for engaging in authorized exports of agricultural commodities, medicine, and medical devices. Following this approach, OFAC applies the licensing procedures required by section 906 of the TSRA to all exports and reexports of agricultural commodities, medicine, and medical devices to Iran that are within the current scope of OFAC's licensing jurisdiction. Similarly, OFAC applies this licensing procedure to cover exports to the government of Iran, any entities in these countries, and individuals in these countries, as well as to persons in third countries purchasing specifically for resale to any of the foregoing.

TSRA is now consolidated within the public-facing Licensing application and information is handled as noted within the Public Licensing application..

f) Sanctions List On-Demand Publishing (T-CLOUD hosted) <https://sanctionslist.ofac.treas.gov/Home/index.html> - The Sanctions List On-Demand publishing application takes raw sanctions list data and converts the data to multiple commonly used structured data file formats (i.e. sdn.csv, sdn.xml, sdn_advanced.xml, etc.) utilized by public end-users. The lists include data about individuals, groups, and entities, such as terrorists and narcotics traffickers designated under sanctions programs. The Sanctions List On-Demand application publishes these lists in a number of human readable formats, as well as formats intended for machine processing and making sanctions lists more generally accessible to the

public.

The Sanctions List Service does not collect any information from site users. It serves as a public dissemination platform only. Its sole function is to provide timely and accurate access to the official OFAC sanctions lists, such as the Specially Designated Nationals (SDN) List and Consolidated Sanctions List.

g) OFAC Administrative System for Investigations and Sanctions (OASIS) (T-CLOUD hosted) <https://ofacweb.wc2h.treasury.gov> - 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), Counsel, Policy Reg, Documents Management System (DMS), General, Global Search, Network Search, OFAC Analytics, OFAC Front Office, Staff Management, Party Management, Template Management, and 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. The SDN module provides OFAC personnel a standardized method for the entry of sanctions list data and automates the creation and publishing of the sanctions lists, including the SDN list, in various formats. OASIS also ingests data from the public facing components that allow the public to submit license applications and submit blocking and reject reports. 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.

The OASIS system is OFAC's official system of record for licensing, compliance, and enforcement activities. It collects and maintains PII from multiple sources to support these functions. The primary source of PII is information submitted directly by the public and regulated entities through OFAC's online portals, including the Licensing application portals and the Online Reporting System (ORS). OASIS also stores PII contained in supporting documentation provided with those submissions, such as contracts, invoices, or identification records, as well as information received through correspondence with applicants or reporting entities. In addition, OASIS may receive PII from financial institutions, other government agencies, and law enforcement agencies in the course of compliance and enforcement activities, as well as from counterparties to reported transactions. Because OASIS serves as the authoritative repository, all such information—whether submitted electronically, in writing, or received through interagency coordination is consolidated in OASIS. Access is restricted to authorized OFAC personnel, and the system is maintained in accordance with Treasury's strict privacy and security requirements. The information collected under the new SCP for PPSIs will also be maintained in OASIS.

h) Reconsideration Portal (TPPS hosted) <https://reconsideration.ofac.treas.gov> – The public facing Reconsideration portal is a customized web-based system that supports the public's ability to request removal from a sanctions list. Petitions for removal

may be submitted by persons designated by OFAC and by their authorized representatives and will include substantiating documentation and verification information related to the removal request. PII is collected and used by OFAC to verify the petitioner and adjudicate the request.

The Reconsideration Portal collects PII from individuals and organizations seeking removal from or changes to OFAC's sanctions lists. Information submitted through the portal may include names, dates of birth, addresses, phone numbers, email addresses, and government-issued identification numbers such as passport or national ID numbers. Applicants may also provide supporting documentation such as financial records, contracts, or identification documents that contain additional PII relevant to their request. In some cases, information about family members, business associates, or counterparties may also be submitted if it supports the reconsideration request. All information collected through the Reconsideration Portal is transmitted securely and stored in OFAC's official system of record, OASIS, where it is accessible only to authorized personnel and protected in accordance with Treasury privacy and security requirements.

i) Disclosure Portal (TPPS hosted) <https://disclosure.ofac.treas.gov> - The public facing Disclosures portal is a customized web-based system that supports the public's ability to disclosure information regarding possible or apparent sanctions violations. PII is collected and used by OFAC to investigate the potential violations of U.S. economic and trade sanctions regulations.

The Disclosure Portal collects PII from individuals and organizations that voluntarily disclose possible or apparent violations of OFAC sanctions programs. Information submitted may include names, dates of birth, addresses, phone numbers, email addresses, and government-issued identification numbers such as passport or national ID numbers. Submissions often include supporting documentation such as financial records, contracts, internal reports, or correspondence that may contain additional PII relevant to the disclosure. Information about employees, counterparties, or other associated individuals may also be provided if it relates to the disclosed conduct. All information collected through the Disclosure Portal is transmitted securely and stored in OFAC's official system of record, OASIS, where it is accessible only to authorized personnel and safeguarded in accordance with Treasury privacy and security requirements.

OFAC maintains PII in OASIS .OFAC collects PII from a variety of individuals in support of its mission to administer and enforce U.S. economic and trade sanctions. This information is processed and maintained in OASIS, which serves as the central repository for PII collected in connection with OFAC's enforcement, licensing, and compliance activities. Individuals who provide PII include members of the public submitting license applications, voluntary self-disclosures, or requests for guidance; representatives of entities subject to OFAC review or enforcement actions; Treasury employees and authorized contractors supporting OFAC operations; and officials from other federal, state, or local agencies involved in interagency coordination or enforcement matters.

PII is collected through several mechanisms. Public-facing electronic submission portals allow

individuals and organizations to submit applications, reports on blocked property or rejected transactions, and other documentation. While some of this information may be temporarily stored in web-based intake systems, it is ultimately transferred to and processed within OASIS. PII may also be obtained through email or written correspondence, voluntary disclosures, third-party complaints, investigative materials, and referrals from other government agencies. All PII is collected and maintained in accordance with applicable federal privacy laws and Treasury policies and is used exclusively for official purposes consistent with OFAC's legal authorities.

Overall, TOS users include Treasury OFAC federal employees, General Counsel staff, and designated consultants and contractors who perform end-user support as well as application-specific system administration, development, and maintenance functions. In addition, TOS users encompass approved external financial institutions accessing ORS, public-facing licensing applicants, and members of the general public who search and review the various sanctions lists.

PII collected and maintained in OASIS is used exclusively to support sanctions case administration. This includes the intake, processing, investigation, documentation, and resolution of matters related to the enforcement and administration of U.S. economic and trade sanctions. OFAC discloses the information in the system to the extent required by the Freedom of Information Act and as allowed by the Privacy Act of 1974 (including the routine uses in the applicable SORN: [**DO .120** - Records Related to Office of Foreign Assets Control Economic Sanctions - 81 FR 78298]).

The sub-applications that support OFAC's mission, such as the Licensing application portals, the OFAC Reporting System (ORS), the Reconsideration Portal, and the Disclosure Portal, serve as mechanisms through which information is submitted to OFAC. These systems may collect content containing PII; however, they operate as conduits to OASIS. All PII submitted through these sub-applications ultimately passes through to OASIS, where it is stored as the official system of record.

OFAC recognizes several inherent privacy risks associated with the collection, use, and disclosure of PII within OASIS. These risks include the potential for unauthorized access or disclosure of sensitive PII to unintended internal or external recipients, either through human error, system misconfiguration, or inadequate access controls. Given that OASIS supports enforcement and compliance operations involving individuals and entities subject to sanctions, the PII collected is often sensitive in nature and may relate to investigations, financial transactions, or legal matters.

There is also a risk of data exposure during electronic transmission, particularly when PII is transferred between systems, shared with other Treasury bureaus, or disseminated to external partners such as other federal agencies. Improper handling or weak encryption during such transmissions could expose PII to interception or unauthorized access. Furthermore, there is a risk that authorized users with access to the system could misuse or exfiltrate data, intentionally or unintentionally, resulting in a breach of privacy or potential identity theft.

Finally, the centralization of large volumes of PII in OASIS creates a potential target for malicious cyber activity, including phishing, intrusion, or insider threats.

OFAC has implemented a comprehensive set of security and privacy controls to protect PII within the OASIS.

As a FISMA High-Impact system and a designated High-Value Asset (HVA), OASIS is subject to the most stringent federal cybersecurity and privacy requirements, designed to ensure the confidentiality, integrity, and availability of sensitive data.
To protect PII during collection, use, and disclosure, OFAC enforces end-to-end encryption for all data transmissions—both internal and external—ensuring that information shared across Treasury bureaus or with authorized external partners is safeguarded against interception or tampering. Within the system, role-based access controls (RBAC) are implemented to ensure that users can access only the minimum necessary information required for their official duties. Access privileges are reviewed and updated regularly to reflect personnel changes and job responsibilities.

In addition, OFAC employs system segmentation, and least privilege principles to limit unnecessary exposure of PII. OASIS also incorporates multi-factor authentication (MFA), system use auditing, and automated logging of all access and activity involving PII, enabling proactive detection of unauthorized or suspicious behavior.

To ensure accountability and oversight, OFAC conducts continuous monitoring of the system environment, including regular privacy impact assessments (PIAs), system security assessments, and internal audits. Users are required to complete annual privacy and cybersecurity training specific to handling high-risk and sensitive information. These measures collectively ensure that the PII in OASIS is protected to the greatest extent practicable in accordance with federal standards, Treasury directives, and the heightened requirements applicable to HVAs.

Section 3.2: 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. The following specific authorities authorize Treasury OFAC System (TOS) collect information:

- 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:
- 31 U.S.C. 321 – General authorities of the Secretary establish the mission of the Department of the Treasury

- 5 U.S.C. 301 – Department 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.

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:

- 31 U.S.C. 321 – General authorities of the Secretary establish the mission of the Department of the Treasury
- 5 U.S.C. 301 – Department 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.

Section 3.3: 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).

Helpful Hint for answering questions in this section and later questions about Privacy Act exemptions: If you know there is a SORN covering the PII in this system, the answer is probably "yes." If the system maintains PII, but that PII is not actually retrieved by a personal identifier, the answer is "no." At the bottom of the applicable SORN(s), you will find a section that says: "Exemptions Claimed for the System." If the answer is "None" (or anything that indicates no exemptions are claimed): (1) your bureau or office does not exempt the system of records from any Privacy Act requirements; and (2) when you are asked in this template whether your bureau or office exempts the system of records from certain provisions in the Privacy Act, your answer will always be "No."
All answers in this section must be provided in the space as instructed after checking the appropriate box(es).

Section 3.3(a) 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. ☐ 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 [choose one] ☐ were ☒ were not required to that SORN. [If modifications were made, generally describe them here]. The current

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:[Provide here the SORN number(s), system of records name(s) and the citation to the SORN(s) in the Federal Register].
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." The citation to the applicable Notice of Proposed Rulemaking and/or Final Rule: **77 FR 28478** (May 15, 2012; Doc. No. 2012-11743).

4: Information Collection: 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 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 4.1(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. ☒ The PII maintained in this system or by this project ***is*** exempt from 5 U.S.C. § 552a(e)(1), because 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 4.1(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. *[Explain **here** what you do to ensure relevance and necessity to the extent possible despite the fact the records are exempt from this 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 4.2 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 *[choose one]* ☒ is ☐ is not 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 [choose one] ☒ is ☐ is not 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 PCLIA updates, this PCLIA will be updated at that time.

Section 4.2: 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	☒ Country or city of residence
	☐ 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)

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	☒ Passport Number and information (nationality, date and place of issuance, and expiration date)
☒ Alien Registration Number	☐ Patient ID Number	☐ 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)	

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

☐ Patient ID Number

☐ Other: (please describe)

Biometrics/Distinguishing Features/Characteristics of Individuals

☐ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) Identify which are collected: (Insert collected here)

☐ Signatures

☐ Palm prints

☐ Fingerprints

☒ Photos/Video: Photos

☐ Voice audio recording

☐ 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 (testing and auditing report, company's name, and point of contact)

Section 4.2 (a) Sources from which PII is obtained

*Focusing on the context in which the data was collected and used (i.e., why it is collected and how it is used), check **ALL** sources from which PII is collected/received and stored in the system or used in the project*

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). OFAC receives information from the public to support the

enforcement of U.S. sanctions programs and to ensure compliance with federal law. Members of the public, including financial institutions, businesses, and individuals, provide information such as reports of potential sanctions violations, requests for licenses, and tips related to sanctioned persons or entities. This input helps OFAC identify and investigate prohibited activities, maintain accurate sanctions lists, and make informed decisions about exemptions or authorizations. By collecting information directly from the public, OFAC strengthens its ability to protect the U.S. financial system, advance national security, and promote the effectiveness of U.S. foreign policy objectives.

☐ 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.

☒ Other: [Explain ***here***]. *In addition to information received from the public, OFAC derives sanctions data from several other key sources that strengthen its ability to design, implement, and enforce sanctions programs. A major source is interagency collaboration, where OFAC works closely with the Department of State, the Department of Justice, the Department of Homeland Security, and the intelligence community to gather classified and law enforcement information on individuals, entities, and activities of concern. OFAC also relies on financial data from domestic and international banking institutions, which provide valuable insights into cross-border transactions, suspicious activity reports, and compliance checks that help uncover sanctions evasion. International partners and allied governments share information that contributes to coordinated sanctions regimes and strengthens multilateral enforcement. In addition, open-source intelligence, such as media reporting, corporate records, and trade data, provides publicly available evidence that can corroborate classified and financial findings.*

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

☐ 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: FinCEN shares information with OFAC derived from Bank Secrecy Act (BSA) reporting and other related financial reporting, which OFAC uses to

identify sanctions evasion, trace illicit financial activity, and support enforcement and designation actions.

4. *Other Federal Agencies*

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

5. *State and Local Agencies*

☒ State and local agencies: OFAC's investigatory and enforcement records may include data from state and local agencies when relevant to sanctions investigations, enforcement actions, or designation reviews. This is explicitly recognized in Treasury's SORNs (System of Records Notices) for OFAC, which list federal, state, local, tribal, and foreign governments as potential sources of information.

6. *Private Sector*

☒ Private sector organizations (for example, banks and financial organizations, data brokers or other commercial sources): *All US financial organizations are legally required to report blocked and rejected transactions. Additionally, OFAC utilizes commercial databases, websites, and corporate filings as part of its investigative process.*

7. *Other Sources*

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

Section 4.3: 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 4.3(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.
2. ☒ Some or ☐ all of the information in this system was collected directly from an individual to whom it pertains.

Section 4.3(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.
2. ☒ Some ☐ All 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 ☒ other .Electronically prior to submission on OFAC sites..
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 4.3(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 4.3(d) Justification of Social Security Numbers

1. ☐ N/A No full SSNs are maintained in the system or by the project. [*Explain if any portion of the SSN short of the full 9 digits is used in the system: Explain]; 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;

☐ 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 4.3(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. ☐ The SSN field is visible, but the SSN itself is blurred or distorted in some way so it is not capable of being read by users who do not require the SSN to perform their official duties.
    c. ☐ 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 and LPRs designated and placed on the SDN list are publicly available. Currently, less than 1% of all targets included on OFAC's sanctions lists include an SSN. In those rare cases, the full SSN is published to assist the public in differentiating designated individuals from others that have similar names and other identifiers. Given that these designated individuals have been essentially cutoff from the US financial system because of their designations as Specially*

Designated Global Terrorists or Specially Designated Narcotics Traffickers, etc., it is extremely unlikely that their publicly available identifiers would be utilized by other bad actors attempting to commit identity fraud. Separately, information provided to OFAC by financial institutions or other US filers under 31 CFR Chapter V may include SSNs. Information included in these blocking and reject reports are kept internally for record and investigative purposes and are not shared with the public in any sort of detailed fashion.

.

Section 4.3(f) Denial of rights, benefits, or privileges for refusing to disclose Social Security Number

1. ☐ N/A 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. If the individual chooses not to provide their SSN. *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 financial institutions sometimes includes the 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. Occasionally, SSNs are collected throughout the course of an investigation by other commercial or law enforcement means.*
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 the right, benefit, or privilege if the individual will be denied if they choose not to provide their SSN: Identify here]. 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 4.3(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).

1. ☐ 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: : *18 U.S.C. 2339B(e), Investigations. The statute authorizes the collection of information during an investigation that might include information about how an individual exercises their First Amendment rights. If this information is submitted voluntarily by US Citizens, LPRs or foreign nationals during an OFAC investigation, it is not entered into OFAC systems because it is not requested or specifically required by OFAC to conduct business.*

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

Section 5.1: 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 5.1(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 the Treasury Privacy Act Handbook 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 5.1(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:
    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 5.1(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 the Treasury Privacy Act Handbook*] .

    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 in addition to information received from the public, OFAC derives sanctions data from several other key sources that strengthen its ability to design, implement, and enforce sanctions programs. A major source is interagency collaboration, where OFAC works closely with the Department of State, the Department of Justice, the Department of Homeland Security, and the intelligence community to gather classified and law enforcement information on individuals, entities, and activities of concern. OFAC also relies on financial data from domestic and international banking institutions, which provide valuable insights into cross-border transactions, suspicious activity reports, and compliance checks that help uncover sanctions evasion. International partners and allied governments share information that contributes to coordinated sanctions regimes and strengthens multilateral enforcement. In addition, open-source intelligence, such as media reporting, corporate records, and trade data, provides publicly available evidence that can corroborate classified and financial findings

        iii. ☐ ***None*** of the records used to make adverse determinations are 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 5.1(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 ☐ are not exempt from the access provisions in the Privacy Act, 5 U.S.C. 552a(d).
   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*]: Descriptions.
   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*]: Description.
   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
   a. ☐ 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 TOS 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 TOS 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 TOS users are only allowed to upload information via web-based access to the ORS and Licensing applications. For ORS, 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 identity provider that makes use of multifactor authentication and identify proofing. The public facing Licensing application allows external TOS 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 TOS database server, TOS internal users further process and verify the data for completeness. A two-way secure shell connection securely transmits information between the TOS web server and the TOS backend database server.

Section 5.2 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 5.2(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.

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 5.3 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 5.3(a) Records in the system used in a computer matching program

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. [*If 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*]: Explain here.

Section 5.3(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.
3. ☐ 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. [discuss **here** the issues that were discovered that required amendment and how those issues are being mitigated/fixed]: Discuss here.

Section 5.3(c) What procedures are followed before adverse action is taken against an individual who is the subject of a matching agreement search?

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

Section 5.4(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 5.4(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).

Section 5.4(c) Making the Accounting of Disclosures Available

1. ☐ 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. ☐ 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: [please state here why the records in this system of records were exempted from this requirement].
4. ☒ 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 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.
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 5.4(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 5.4(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.

Section 6: Compliance with Federal information management requirements

Responses to the questions below address the practical, policy, and legal consequences of failing to comply with one or more of the following federal information management requirements (to the extent required) and how those risks were or are being mitigated: (1) the Privacy Act System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Gov Act security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

Section 6.1: 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 6.1(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 is submitting to OMB an Information Collection Request ("ICR") related to the specific, new information collection requirements for the Sanctions Compliance Program (SCP) for PPSIs and is waiting for OMB approval in conjunction with the proposed new regulation. OFAC's current OMB Control Numbers are: 1505-0164 (Reporting, Procedures, and Penalties Regulations) and 1505-0198 (Rough Diamonds). OMB Control Number 1505-0231 is the parent control number for OFAC's Website User Survey conducted in September 2024.
4. ☐ The project or system did not complete an Information Collection Request ("ICR") and receive OMB approval because it is exempt from PRA.

Section 6.2: 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 6.2(a)

1. ☒ The records used in the system or by the project are covered by a NARA's General Records Schedule (GRS). The GRS is The OFAC schedule governing these documents is GRS 3.1 (items 001, 010, 011, 020, 030), GRS 3.2, GRS 5.2, and GRS 6.3 (Items 010 and 020).

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]*.
4. ☒ The system owner is still in the process of developing a new records schedule to submit to NARA.

Section 6.3: 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 6.3(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: 7/21/2022 (ATO currently in the process of being converted to continuous ATO).
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 6.4: 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 6.4(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)? *If checked:*
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.
4. ☐ The system or project is not in compliance with all Section 508 requirements. The following actions are in progress to ensure compliance: [please describe here the efforts underway to ensure compliance*]*.

Responsible Officials Certification

☐ A PCLIA is being completed for this system for the first time. I have reviewed all responses in the PCLIA and it reflects the current, accurate, and complete status of the system, including the significant changes.

☒ This system was reviewed pursuant to continuous monitoring requirements. Since the PCLIA was last updated, significant changes have been made to the system that warranted modifications to the PCLIA. I have reviewed all responses in the PCLIA and it reflects the current, accurate, and complete status of the system, including the significant changes.

☐ This system was reviewed pursuant to continuous monitoring requirements. Since the PCLIA was last updated, **no** significant changes have been made to the system that would warrant any modifications to the PCLIA. I have reviewed all responses in the PCLIA and it reflects the current, accurate, and complete status of the system.

Aaron Mintz
TOS System Owner
Office of Foreign Assets Control

Dennis Blount
TOS System Owner Designated Representative
Departmental Offices, & Records

Approval Signature

_____

Ryan Law
Deputy Assistant Secretary
Departmental Offices, & Records