Privacy and Civil Liberties Impact Assessment
for the

THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES TREASURY MICROSOFT DYNAMICS SYSTEM AND TREASURY SECURE DATA NETWORK (TOGETHER, THE CASE MANAGEMENT SYSTEM)

December 1, 2020

Reviewing Official
Ryan Law
Deputy Assistant Secretary for Privacy, Transparency, and Records
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 for unclassified systems when PII is maintained in a system or by a project. This PCLIA provides the following information regarding the system or project: (1) an overview of its purpose and functions; (2) a description of the information collected; (3) a description of the how information is maintained, used, and shared; (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and (5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

Section 2: System Overview

Section 2.1: System/Project Description and Purpose

The Committee on Foreign Investment in the United States (CFIUS) is an inter-agency committee authorized to assess, review and investigate transactions that could result in control of a U.S. business by a foreign person and certain non-controlling investments and real estate transactions involving foreign persons, in order to determine the effect of such transactions on the national security of the United States. CFIUS uses the Case Management System in order to collect information submitted by the parties to transactions assessed, reviewed or investigated by CFIUS and other available information related to such transactions, and disseminate such information to certain Executive Branch agencies to coordinate CFIUS's national security functions related to such transactions.

The members of CFIUS include the heads of the following departments and offices: (1) Department of the Treasury (chair); (2) Department of Justice; (3) Department of Homeland Security; (4) Department of Commerce; (5) Department of Defense; (6) Department of State; (7) Department of Energy; (8) Office of the U.S. Trade Representative; and (9) Office of Science & Technology Policy. The following offices also observe and, as appropriate, participate in CFIUS's activities: (1) Office of Management & Budget; (2) Council of Economic Advisors; (3) National Security Council; (4) National Economic Council; and (5) Homeland Security Council. The Director of National Intelligence and the Secretary of Labor are non-voting, ex-officio members of CFIUS with roles as defined by statute and regulation.

The CFIUS program operates in both classified and unclassified environments. Treasury typically does not conduct and publicly post PCLIAs for classified systems. This PCLIA covers

only the unclassified environment, but provides information regarding the classified CFIUS environment to the extent the information is already public and as necessary to explain the data flows between the classified and unclassified environments.

1. ☐ A PCLIA is being done for this system for the first time.
2. ☒ This is an update of a PCLIA previously completed and published under this same system or project name. The date the earlier PCLIA was published was May 20, 2020.
3. ☐ This is an update of a PCLIA previously completed and published for a similar system or project that is undergoing a substantial modification or migration to a new system or project name.

Section 2.2: Authority to Collect

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

31 U.S.C. 321; 5 U.S.C. 301; 50 U.S.C. 4565; 44 U.S.C. 3101; E.O. 9397, 11858, 12333, 12968, 13478, and 13526, as amended; 31 CFR Part 800 (2019); 31 CFR Parts 800-802 (2020), as amended.

Section 2.3: Privacy Act Applicability; SORN Requirement

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

Section 2.3(a)

1. ☐ A SORN is not required.
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. The current applicable SORN is: ***here***
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) will be published on the Treasury website: *https://home.treasury.gov/footer/privacy-act/system-of-records-notices-sorns*
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): *5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H),and (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).*

Section 3: Information Collection

Section 3.1: Relevant and Necessary

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

Section 3.1(a) Exemption Claimed from this Requirement.

1. ☐ The PII maintained in this system or by this project is **not** exempt from 5 U.S.C. § 552a(e)(1), the Privacy Act's requirement that an agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."

   ☒ The PII maintained in this system or by this project **is** exempt from *5 U.S.C. § 552a(e)(1) because Treasury claimed exemptions under 5 U.S.C. 552a(k)(1) and (k)(2). The CFIUS program makes every effort to maintain only records that are necessary and relevant to its mission. In the course of its operations, however, CFIUS must be able to review information from a variety of sources. What information is relevant and necessary may not always be apparent until after the evaluation is completed. In the interests of national security, it is appropriate to include a broad range of information that may aid in identifying and assessing the nature and scope of potential threats to the United States*.
2. ☐ The PII is not maintained in a system of records. Therefore, the Privacy Act relevance and necessity requirements do not apply.

Section 3.1(b) Continuously Assessing Relevance and Necessity

1. ☐ The PII in the system is not maintained in a system of records.
2. ☐ Although the records are not maintained in a system of records, the program did conduct an assessment prior to collecting PII for use in the system or project to determine which PII data elements and types (see Section 3.2 below) were relevant and necessary to meet the system's or project's mission requirements. 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 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

3. ☒ 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 limited to only that which is relevant and necessary to meet the system's or project's mission requirements (subject to the limitation stated in response to Section 3.1(a)(1) above). During the PCLIA process (including future updates), Treasury reviews the system to ensure the continuing relevance and necessity of the PII to the fullest extent possible.
4. ☒ 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 3.2: PII and/or information types or groupings

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

Biographical/general information		
☒ Name	☒ Nationality	☒ Country/Place of Birth
☐ Age	☒ Citizenship	☐ Immigration Status
☒ Date of birth	☐ Ethnicity	☒ Alias (including nicknames and all other names used)
☐ Home physical/postal mailing address	☐ Gender	☒ City or County of Birth
☐ Zip Code	☐ Race	☒ Military Service Information
☐ Personal home phone, cell phone, or fax number	☐ Personal e-mail address	☐ Other (please describe):
☒ Country or city of residence	☐ Other (please describe):	☐ Other (please describe):
Other information		
☒ Resume, curriculum vitae or other professional synopsis	☐ Cubicle 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 (only if voluntarily submitted in curriculum vitae)	☐ Information about children	☐ Other (please describe):
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe):
Identifying numbers assigned to individuals		
☒ Full Social Security number	☐ Personal device identifiers or serial numbers	☐ Vehicle Identification Number
☐ Truncated Social Security Number (e.g., last 4 digits)	☐ Internet Protocol (IP) Address	☐ Driver's License Number
☐ Employee Identification Number	☐ Personal Bank Account Number	☐ License Plate Number
☐ Taxpayer Identification Number	☐ Health Plan Beneficiary Number	☐ Professional License Number
☐ File/Case ID Number	☐ Credit Card Number	☒ Other Identifying Numbers (please describe): National Identity Number including nationality, date and place of issuance, and expiration date (where applicable)
☐ Alien Registration Number	☐ Patient ID Number	☒ Other Identifying Numbers: U.S. visa holder information, including visa type and number, date and place of issuance, and expiration date).
☒ Passport Number (U.S. and Foreign) (nationality, date and place of issuance, and expiration date	☐ Other (please describe):	☐ Other (please describe):
Specific Information/File Types		
☐ Taxpayer Information/Tax Return Information	☐ Law Enforcement Information	☐ Security Clearance/Background Check Information
☒ Civil/Criminal History Information/Police Records (obtained from government source)	☒ Civil/Criminal History Information/Police Records (obtained from commercial source)	☐ Credit History Information (government source)
☐ Protected Information (as defined in Treasury Directive 25-10)	☐ Credit History Information (commercial source)	☐ Bank Secrecy Act Information
☐ Information provided under a confidentiality agreement	☐ Case files	☐ Personnel Files
☐ Business Financial Information (including loan information)	☐ Personal Financial Information (e.g., loan information)	☐ Information subject to the terms of an international or other agreement
☒ Passport information (state which passport data elements are collected if not all)	☐ Other (please describe): _____	☐ Other (please describe): _____
Audit Log and Security Monitoring Information		
☒ User ID assigned to or generated by a user of Treasury IT (including system activity associated with that User ID)	☐ 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_____	☐ Other_____	☐ Other_____
Biometrics/Distinguishing Features/Characteristics of Individuals		
☐ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) Identify which are collected: _____	☐ Signatures	☐ Palm prints
☐ Fingerprints	☐ Photos/Video (identify which: _____)	☐ Voice audio recording
☐ Other (please describe): _____	☐ Other (please describe): _____	☐ Other (please describe): _____
Identifying numbers for sole proprietors (including business information).		
☐ Sole proprietor business credit card number	☐ Business Phone or Fax Number	☐ Business Physical/Postal Mailing Address
☐ Sole proprietor business professional license number	☐ Sole proprietor business file case number	☐ Sole proprietor business taxpayer identification number
☐ Sole proprietor business license plate number	☐ Sole proprietor business vehicle identification number	☐ Sole proprietor business bank account number
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe):

3.3 Sources from which PII is obtained

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:

☒ Members of the general public (current association with the federal government, if any, is irrelevant to the collection and use of the information). *Parties to transactions filed with CFIUS submit PII to CFIUS; submission of such transactions is voluntary except as required to comply with mandatory declaration requirements for certain types of transactions. The PII relates to persons associated with the foreign person engaged in the transaction (which could include US citizens or lawful permanent residents) and certain parent entities (e.g., for purposes of conducting background checks) which informs CFIUS's determination of the effects of a transaction on the national security of the United States. The PII also includes contact information for the US businesses and foreign persons that are parties to, or, in applicable cases, the subject of, the transaction.*

☐ Federal employees in their personal capacity (information unrelated to federal work/employment).

☐ Current federal employees

☐ Retired federal employees (only check if relevant to the purpose for collecting and using the information).

☐ Former Treasury employees (only check if relevant to the purpose for collecting and using the information).

☐ Federal contractors, grantees, interns, detailees etc. (current or former) (only check if relevant to the purpose for collecting and using the information).

☐ Federal job applicants (only check if relevant to the purpose for collecting and using the information).

☒ Other: *Foreign persons whose "biographical" and "personal identifier information" are relevant to a transaction filed with CFIUS.*

2. Current Federal Employees, Interns, and Detailees

☐ Current Federal employees providing information in their capacity as federal employees (for example, OPM or Treasury forms related to employment with the federal government) (this would not include individuals who are current federal employees completing a form in their "personal" capacity [e.g., their personal tax forms or seeking some federal benefit available to the general public in their personal capacity]). Current federal employees acting in their personal capacity are treated as "Members of the general public"). If current federal employee's information is in the system in both their personal and official capacity, check both this box and "members of the public" if not already checked above.

☐ Interns

☐ Detailees

☐ Other employment-related positions: [describe here].

3. Treasury Bureaus (including Departmental Offices)

☐ Other Treasury Bureaus: [name the bureau(s) here and identify the bureau/office information system from which the PII originated)].

4. Other Federal Agencies

   ☒ Other federal agencies*: Any federal agency that is a member of CFIUS can submit information related to a transaction that falls within CFIUS's jurisdiction.*

5. State and Local Agencies

   ☐ State and local agencies: [name the State and local agencies here].

6. Private Sector

   ☒ *Any "foreign person" (as defined in the CFIUS regulations) who is party to a transaction filed with CFIUS can submit PII on behalf of its employees or itself. Those employees may include United States citizens and lawful permanent residents. The PII also includes contact information for the US businesses and foreign persons party to, or, in applicable cases, the subject of, the transaction, which may be submitted by the US businesses or foreign persons party to the transaction.*

7. Other Sources

   ☒ Other sources not covered above: *The CFIUS program receives information from the notifying party or parties regarding any transaction that could result in foreign control of any U.S. business and certain non-controlling investments and real estate transaction. CFIUS reviews or assesses, and may subsequently investigate, to determine the effects of such transactions on the national security of the United States. The notifying party could be submitting the information on behalf of all parties to the transaction, or a member of the public could be notifying CFIUS because of concerns that a transaction may affect national security. In certain cases, the individual submitting documents on behalf of the notifying party may also be submitting their own PII (e.g., curriculum vitae) in addition to other information that must be submitted for the notifying parties to obtain the benefits of safe harbor.*

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

When Federal agencies request information from an individual that will be maintained in a system of records, they must inform the individual of the following: "(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on [the individual], if any, of not providing all or any part of the requested information." 5 U.S.C § 522a(e)(3). This is commonly called a Privacy Act Statement. The OMB Guidelines also note that subsection (e)(3) is applicable to both written and oral (i.e., interview) solicitations of personal information. Therefore, even if a federal employee or contractor has a fixed list of questions that they orally ask the individual in order to collect their information, this requirement applies.

Section 3.3(a)

1. ☐ None of the PII in the system was collected directly from an individual (US Citizen or lawful permanent resident) to whom it pertains.

2. ☒ Some or ☐ all of the information in this system was collected directly from an individual to whom it pertains. *In most situations, the CFIUS program receives information from the notifying party (or parties) regarding transactions subject to CFIUS review. Information regarding foreign nationals, US Citizens, and lawful permanent residents involved in a transaction is obtained from the relevant notifying party and/or directly from the foreign national. PII typically is not collected directly from the US Citizens or lawful permanent residents to whom it pertains. In certain cases, however, the individual submitting documents on behalf of the notifying party may also be submitting their own PII (e.g., curriculum vitae) in addition to other information that must be submitted for the notifying parties to potentially obtain the benefits of safe harbor.*

Section 3.3(b)

1. ☐ Some of the PII in the system was collected directly from the individuals (US Citizen or lawful permanent resident) to whom it pertains.
2. ☒ Some ☐ All of the PII in the system was collected directly from the individual to whom it pertains for the purpose of entering it into a system of records. Therefore, a Privacy Act Statement is provided on the CFIUS website at the point where the submitting party logs into the system to provide PII relevant to a particular transaction.
3. The Privacy Act Statement contained the following:
    a. ☐ *A Privacy Act Statement is not required because the program does not maintain a system of records.*
    b. ☒ The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
    c. ☒ Whether disclosure of such information is mandatory or voluntary.
    d. ☒ The principal purpose or purposes for which the information is intended to be used.
    e. ☒ The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
    f. ☒ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

Section 3.3(c) Use of Full Social Security Numbers

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

Section 3.3(d) Justification Social Security Numbers

1. ☐ N/A No full SSNs are maintained in the system or by the project.

2. ☒ Full SSNs are maintained in the system or by the project and the following approved Treasury uses of SSNs apply: *Full SSNs are specifically required by 31 C.F.R. § 800.502 and 31 C.F.R. § 802.502, and are part of a larger body of data considered when analyzing covered transactions from a national security and intelligence perspective. Treasury allows the collection of SSNs for law enforcement and intelligence purposes. Treasury also allows SSN collection where required by law or regulation.*

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

1. ☐ Full SSNs are ***not*** maintained in the system or by the project.
2. ☐ Only partial SSNs are maintained in the system or by the project. The numbers from the SSN that are visible are [explain ***here***] [e.g., the last four or last five numbers in the SSN]. The full SSN is maintained in a separate system, [name the system ***here***].
3. ☒ 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. ☐ Some employees who have access to the SSN do not require the full SSN to perform their official duties. ☐ Within the system, an alternative number (e.g., an Employee ID) is displayed to all system users who do not require the SSN to perform their official duties. The SSN is only linked to the alternative number within the system and when reporting outside the system (to an agency that requires the full SSN). The SSN is not visible to system users (other than administrators).
    c. ☐ 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.
    d. ☐ 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).
    e. ☒ Other: *The full SSNs are removed from the unclassified system (the Treasury Microsoft Dynamics System) and uploaded to the Treasury Secure Data Network (TSDN), a Treasury system that maintains classified information up to the level of "Secret." The additional security provided on the classified system and strict application of access and "need-to-know" requirements reduces the risk associated with maintaining the SSN.*

Section 3.3(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 or organization chooses not to provide the SSN, a voluntary notice is incomplete. CFIUS cannot begin reviews of incomplete voluntary notices, and the CFIUS regulations prohibit the CFIUS Staff Chair from waiving the PII requirements for voluntary notices. Therefore, if a party or parties to a transaction file a voluntary notice with CFIUS in order to seek regulatory safe harbor for their transaction, but also refuse to provide SSNs, CFIUS will not begin the review process that may grant such safe harbor. This does not violate the law because:*☒ *SSN disclosure is required by the following Federal statute, Executive Order or regulation: 31 C.F.R. § 800.502 and 802.502.*

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

The Privacy Act requires that Federal agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

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 ***might*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment. *If you checked this box, please check the correct box below:*

    a. ☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.

    b. ☒ The information maintained is pertinent to and within the scope of an authorized law enforcement or intelligence activity. *The CFIUS regulations require submission of a "curriculum vitae [CV] or similar professional synopsis as part of the notice" for "each member of the board of directors and each officer of the foreign person engaged in the transaction and its immediate, intermediate, and ultimate parents (see § 800.219 for the definition of ''parent''), and for any individual having an ownership interest of five percent or more in the foreign person engaged in the transaction and in its ultimate parent." CFIUS will collect some of these CVs or other professional synopses (collectively "CV") about U.S. citizens and lawful permanent residents ("individuals" under the Privacy Act) (and on some occasions, directly from the individual about whom the CV is written). The contents of a CV will vary depending on the individual's personal choices or requirements, but some of these CVs may include information about organizations in which the individual is a member. This type of*

information is not requested or specifically required by CFIUS, but an individual could conceivably submit this information voluntarily in a CV.

c. ☐ The following statute expressly authorizes its collection.

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

Section 4.1: How is the information collected used?

The information collected and maintained in the system is used to determine if the proposed transaction is subject to CFIUS's jurisdiction, and the effect of such transaction on the national security of the United States. The specific PII elements and how they are used are as follows:

- *The "name" is used to determine the identity of the individual(s) involved in the transaction. Use of this information is consistent with the program's statutory authority.*
- *The "date of birth" is used to identify the individual(s) involved in the transaction. Use of this information is consistent with the program's statutory authority.*
- *The "military service information (foreign country)" is useful for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *The "alias (including nicknames and all other names used)" of the applicant is used to further identify the individual(s) involved in the transaction. Use of this information is consistent with the program's statutory authority.*
- *The "business physical/postal mailing address" is used to analyze the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *The "nationality" and "citizenship" are used to analyze the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *The "resume or curriculum vitae" is used for further identification of the individual involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *The "country and city of residence" is used for further identification of the individual involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *The "place of birth" is used to identify the individual(s) involved in the transaction. Use of this information is consistent with the program's statutory authority.*
- *The "full social security number" is used to further identify the individual(s) involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *The "national identity number, including nationality, date and place of issuance, and expiration date" are used to further identify the individual(s) involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*

- *The "passport number" is used to further identify the individual(s) involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *"U.S. visa holder information" is used to further identify the individual(s) involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *"Group/organization information" is used to further identify the individual(s) involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*
- *"User ID assigned to or generated by a user of Treasury IT (including system activity associated with that User ID)" is used to further identify the individual(s) involved in the transaction. Use of this information is consistent with the program's statutory authority.*
- *Civil/Criminal History Information/Police Records are used to further identify the individual(s) involved in the transaction, and for analyzing the potential effects of the transaction on the national security of the United States. Use of this information is consistent with the program's statutory authority.*

Section 4.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared when it is used to make determinations about individuals

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

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

Section 4.2(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. *However, CFIUS does not make determinations about individuals. Determinations are made about transactions. Notifying parties provide information regarding transactions that involve a U.S. business or real estate in the United States and a foreign person (an individual or entity). A decision by CFIUS to impose conditions on a transaction or to refer a transaction to the President for potentially adverse action could, however, have a secondary effect on individuals who have some personal interest in the completion of the transaction. When notifying parties submit a transaction for review, they are required to provide the information required by the regulations. This includes the information the individual possesses regarding foreign nationals and individuals (including US citizens and lawful permanent residents) who are involved in the transaction. Notifying parties may come forward at any time to provide updated information or to correct information previously provided if requested by CFIUS staff in the course of CFIUS reviews. CFIUS allows parties to submit additional information at any time.*

2. ☐ All ☐ Some of the PII maintained in the system or by the project is part of a system of records and ***is*** exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act. The exemption claimed for these records is appropriate because *[please see Appendix B which contains sample justifications for this exemption and provide the appropriate bases **here** [more than one bases may apply]].*
3. ☐ The PII maintained in the system or by the project is ***not*** part of a system of records as defined in section (e)(5) of the Privacy Act; and is ***not*** (b) used to make any determinations about individuals.

Section 4.2(b) Protections in place despite exemption from the accuracy, relevance, timeliness, and completeness requirements

1. ☐ *The system does not maintain a system of records. Therefore, this requirement does not apply.*
2. ☒ **None** *o*f 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. *However, CFIUS does not make determinations about individuals. Determinations are made about transactions. Notifying parties provide information regarding transactions that involve a U.S. business or real estate in the United States and a foreign person (an individual or entity). A decision by CFIUS to impose conditions on a transaction or to refer a transaction to the President for potentially adverse action could, however, have a secondary effect on individuals who have some personal interest in the completion of the transaction. When notifying parties submit a transaction for review, they are required to provide the information required by the regulations. This includes the information the individual possesses regarding foreign nationals and individuals (including US citizens and lawful permanent residents) who are involved in the transaction. Notifying parties may come forward at any time to provide updated information or to correct information previously provided if requested by CFIUS staff in the course of CFIUS reviews. CFIUS allows parties to submit additional information at any time.*

3. ☐ For all information maintained in the system or by the project that is part of a system of records that is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act, the following efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible without interfering with the (*check one*) ☐ law enforcement ☐ intelligence ☐ other [*describe **here***] mission requirements for which the system or project was created [*choose **ALL** that apply*]:
    a. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals.
    b. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals without additional research and investigation to ensure accuracy, relevance, timeliness, and completeness.
    c. ☐ Individuals and organizations to whom PII from the system or project is disclosed (as authorized by the Privacy Act) determine its accuracy, relevance, timeliness, and completeness in a manner reasonable for their purposes before they use it to make adverse determinations about individuals.
    d. ☐ Individuals about whom adverse determinations are made using PII from this system or project are given an opportunity to explain or modify their information (*check one*) ☐ before ☐ after the adverse determination is made. During this process, individuals are allowed to: [*discuss **here***
    e. ☐ Other: (*please describe*):
4. ☐ No additional efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible because it would interfere with mission requirements.

Section 4.2(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 "*collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs*." Agencies may exempt a system of records from this requirement under certain circumstances and if certain conditions are met.

5. ☒ *The records in the CFIUS system are not used to make adverse determinations about individuals. Determinations are made about transactions. Notifying parties provide information regarding transactions that involve a U.S. business or real estate in the United States and a foreign person (an individual or entity). A decision by CFIUS to impose conditions on a transaction or to refer a transaction to the President for potentially adverse action could, however, have a secondary effect on individuals who have some personal interest in the completion of the transaction. When notifying parties submit a transaction for review, they are required to provide the information required by the regulations. This includes the information the individual possesses regarding foreign nationals and individuals (including US citizens and lawful permanent residents)*

who are involved in the transaction. Notifying parties may come forward at any time to provide updated information or to correct information previously provided if requested by CFIUS staff in the course of CFIUS reviews. CFIUS allows parties to submit additional information at any time.

☐ 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. ☐ 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 [*please explain **here** why third-party data is required to make this determination; e.g., third-party data is required to verify the accuracy of the information provided by the individual seeking a privilege or benefit].*

ii. ☐ ***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 4.2(d) Additional controls designed to ensure accuracy, completeness, timeliness and fairness to individuals in making adverse determinations

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. *Nevertheless, submitting organizations may update the information they submitted at any time.*

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, but the Act does not

apply to CFIUS. *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.
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.
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***].

Technical controls. The system or project can also employ 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:

☐ Additional technical controls are not employed in this system or project because:

a. ☐ Not applicable. Additional technical controls are employed.
b. ☐ 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.
c. ☐ 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).

☒ Additional technical controls are employed in this system or project. The additional technical controls are as follows:

a. ☐ No additional technical controls are available to ensure accuracy, relevance, timeliness and completeness. [Explain here why no additional technical controls are available (e.g., system updates would be required and funding is not available)].
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: *After CFIUS determines that the contents of a file submitted for review meet the legal requirements, the file is removed from the unclassified system (the Treasury Microsoft Dynamics System) and uploaded to TSDN, a Treasury system that maintains classified information up to the level of "Secret." The additional security provided on the classified system, including system and file access controls, and strict application of "need-to-know" requirements, reduces the risk associated with maintaining the information.*

Section 4.3 Data-Mining

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

Section 4.3(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 4.4 Computer Matching

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

Pursuant to the CMPPA, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The

second type of matching program involves the computerized comparison of two or more automated systems of records or a system of records with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8).

Matching programs must be conducted pursuant to a matching agreement between the source (the agency providing the records) and recipient agency (the agency that receives and uses the records to make determinations). The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

Section 4.4(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. [*Explain **here** whether a Matching Agreement was executed and published as required by the CMPPA/Privacy Act; if no Matching Agreement was executed, please explain here why*].

Section 4.4(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.

Section 4.4(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 4.5: Information sharing with external (i.e., outside Treasury) organizations and individuals

Section 4.5(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 as follows with agencies, organizations, or individuals external to Treasury:

After completion of the initial CFIUS intake process on the Treasury Microsoft Dynamics System, PII is moved to the classified TSDN environment and shared with certain Executive Branch agencies.
This information is shared in order to determine whether a transaction is subject to CFIUS's jurisdiction and to facilitate a robust analysis of transactions subject to CFIUS's jurisdiction to ensure that these transactions will not impair the national security of the United States or pose unresolved national security concerns (as required in applicable CFIUS legislation and other federal laws).

Privacy risks are mitigated through the use of an encrypted Web portal for submission of PII to CFIUS and/or via encrypted emails sent to Treasury as necessary. The data is protected in the unclassified case management system by Treasury's cybersecurity policies as directed by Treasury Directive 85-01, Department of the Treasury Information Technology Security Program. An increased level of security is achieved once the case file is moved to the classified TSDN environment.

3. ☐ All external disclosures ***are*** authorized by the Privacy Act (including routine uses in the applicable SORN).

Section 4.5(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 4.5(c) Making the Accounting of Disclosures Available

1. ☒ *CFIUS exempted this system of records from this requirement under exemptions (k)(1) and (k)(2). Release of the accounting of disclosures of the records in this system could alert individuals that they have been identified as a national security threat or the subject of an analysis related to the national security interests of the United States, to the existence of the analysis, and reveal the interest on the part of Treasury or CFIUS as well as the recipient agency. Disclosure of the accounting would present a serious impediment to efforts to protect national security interests by giving individuals an opportunity to learn whether they have been identified as subjects of a national security-related analysis and take steps to impede the analysis and avoid detection, including (i) taking steps to avoid analysis, (ii) informing associates that a national security analysis is in progress, (iii) learning the nature of the national security analysis, (iv) learning the scope of the national security analysis, (v) beginning, continuing, or resuming conduct that may pose a threat to national security upon inferring they may not be part of a national security analysis because their records were not disclosed, or (vi) destroying information relevant to a national security analysis.*
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 ***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.
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 ***not*** maintained regularly, but is capable of being constructed in a reasonable amount of time upon request. The information necessary to reconstruct the log (i.e., date, nature, and purpose of each disclosure) is maintained for at least five years.

Section 4.5(d) Obtaining Consent Prior to New Disclosures Not Authorized by the Privacy Act

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

Section 4.5(e) Obtaining Prior Written Consent.

1. ☐ The records are not maintained in a system of records. Therefore, this Privacy Act requirement does not apply.
2. ☒ 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.
3. ☒ 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 5: Compliance with federal information management requirements

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

Section 5.1: The Paperwork Reduction Act

The PRA requires OMB approval before a Federal agency may collect standardized data from 10 or more respondents within a 12-month period. OMB also requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

Section 5.1(a)

1. ☒ The system or project maintains information obtained from individuals and/or organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government).
2. ☒ The project or system involves a new collection of information in identifiable form for 10 or more persons from outside the federal government.
3. ☒ The project or system completed an Information Collection Request ("ICR") and received OMB approval. The OMB Control Number for the approved collection is *1505-0121*.
4. ☐ The project or system did not complete an Information Collection Request ("ICR") and receive OMB approval because [explain here why an ICR is either not required or provide the status on completing the ICR and OMB approval].

Section 5.2: Records Management - NARA/Federal Records Act Requirements

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the National Archives and Records Administration (NARA) for permanent retention upon expiration of this period. If the system has an applicable SORN(s), check the "Policies and Practices for Retention and Disposal of Records" section.

Section 5.2(a)

1. ☐ The records used in the system or by the project are covered by a NARA's General Records Schedule (GRS). The GRS is *[please provide **here** the general schedule name and identifying number].*
2. ☒ The records used in the system or by the project are covered by a NARA approved Treasury bureau Specific Records Schedule (SRS): *Treasury RS N1-056-03-10 item 1a.*
3. ☐ On [*please state the date on which NARA approval was sought*] the system owner sought approval from NARA for an SRS and is awaiting a response from NARA. *[State **here** the retention periods you proposed to NARA*].

Section 5.3: E-Government Act/NIST Compliance

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

Section 5.3(a)

1. ☒ The system is a federal information system subject to FISMA requirements.
2. ☒ The system last completed an SA&A and received an ATO on: May 20, 2020.
3. ☐This is a new system has not yet been authorized to operate. The expected to date for receiving ATO is *[please state **here** the expected date on which you expect authorization will be granted].*
4. ☒The system or project maintains access controls to ensure that access to PII maintained is limited to individuals who have a need to know the information in order to perform their official Treasury duties.
5. ☒ All Treasury/bureau security requirements are met when disclosing and transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury system or project to internal or external parties.
6. ☒ This system or project maintains an audit log of system users to ensure they do not violate the system and/or Treasury/bureau rules of behavior.
7. ☐ This system or project has the capability to identify, locate, and monitor individuals or groups of people other than the monitoring of system users to ensure that they do not violate the system's rules of behavior. *[If checked, please describe this capability **here**, including safeguards put in place to ensure the protection of privacy and civil liberties.]*

Section 5.4: Section 508 of the Rehabilitation Act of 1973

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

Section 5.4(a)

1. ☐ The project or system will ***not*** involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)?
2. ☒The project or system ***will*** involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)? *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

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

Approval Signature

_____

Ryan Law
Deputy Assistant Secretary for Privacy, Transparency, and Records