Privacy and Civil Liberties Impact Assessment

Template version 5.0

Enterprise Service Management (ESM) ServiceNow

July 6th, 2022

Bureau Certifying Official

David J. Ambrose

Chief Security Officer and Chief Privacy Officer

Bureau of the Fiscal Service

Department of the Treasury

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy and Civil Liberties Impact Assessment (PCLIA) is a public document and will be made available to the general public via the Fiscal Service Privacy and Civil Liberties Impact Assessment (PCLIA) webpage (https://www.fiscal.treasury.gov/pia.html).

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 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 purpose of the Enterprise Service Management (ESM) ServiceNow is to provide workflow application for IT Service Management process, Case management for Travel, HR, and Fiscal Accounting requests, A workflow application for the risk management framework process supporting FIMSA systems and Human Resources related document management and workflows.

PII is used to identify and authenticate users. This data is stored in the system long term. Through HR request processing PII is collected to perform HR related requests. This PII is introduced into the system via documents. These documents are stored with the case. Once the HR case is closed for 90 days the attachments are removed.

It supports the mission of the Bureau by providing a ticketing and case management solution that supports multiple business areas including Payments, Debt Management, Retail Security Services, Management, Information and Security Services, Revenue Collection Management, Office of Shared Services, and Fiscal Accounting.

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.

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 information may also be collected pursuant to a more general requirement or authority.

The following specific authorities authorize Treasury/Bureau of the Fiscal Service to collect the information maintained in this system:

Homeland Security Presidential Directive 12 (HSPD-12)
Federal Information Processing Standard 201: Policy for a common Identification Standard for Federal Employees and Contractors.

Specific to HR related records is 5 USC 301; 40 USC 581; 31 USC chapter 33; 31 USC 3720; US office of personnel management, Guide to Personal Recordkeeping (Operating Manual)

Section 2.3: Privacy Act Applicability; SORN Requirement

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

Section 2.3(a)

1. ☐ The system or project does **not** retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. **A SORN is not required** with respect to the records in this system.

2. ☒ The system or project **does** retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual.
   A SORN is required with respect to the records in this system.

3. ☐ A SORN was identified in the original PCLIA and a determination was made during this current PCLIA update that modifications (☐ were ☐ were not) required to that SORN

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.

5. ☐ A SORN was published and no exemptions are taken from any Privacy Act requirements.

6. ☐ Exemptions are claimed from the Privacy Act provisions in the applicable SORN(s).

The following are the Privacy Act systems of records notices **(SORN)**s that cover the records maintained in this system:

List all applicable SORN(s) **here:**
Treasury .015
Fiscal Service .005
OPM/GOVT -1
OPM/GOVT -2
OPM/GOVT -3
OPM/GOVT -5
OPM/GOVT -6
OPM/GOVT -7
OPM/GOVT -9
OPM/GOVT -10

Section 3: Information Collection

Section 3.1: Relevant and Necessary

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

Section 3.1(a) Exemption Claimed from this Requirement.

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

2. ☐ The PII maintained in this system or by this project **is** exempt from 5 U.S.C. § 552a(e)(1).

Section 3.1(b) Continuously Assessing Relevance and Necessity

1. ☐ The PII in the system is not maintained in a system of records. Therefore, the Privacy requirements do not apply.

2. ☐ The PII in the system is maintained in a system of records, but the agency exempted these records from the relevance and necessity requirement.

3. ☒ The system owner conducted an assessment prior to collecting PII for use in the system or project to determine which PII data elements and types (reference the **PII Holdings Survey**) were relevant and necessary to meet the system's or project's mission requirements.

   In conducting the current "relevance and necessity" analysis that is documented in this PCLIA, the system owners reevaluated the necessity and relevance of all PII and determined that the data elements currently maintained 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 is no longer relevant or necessary, the system owner will cease using the PII and update this PCLIA to discuss how the data element was removed from the system and is no longer used or collected.

4. ☒ With respect to PII currently maintained in the system or by the project, the PII (☒ 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 (☒ is ☐ is not) a process in place to continuously reevaluate and ensure that the PII remains relevant and necessary.

Section 3.2 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):
   a. ☐ 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).
   b. ☐ Retired federal employees.
   c. ☐ Former Fiscal Service employees.
   d. ☒ Federal contractors, grantees, interns, detailees etc.
   e. ☒ Federal job applicants.
   f. ☐ Other:

2. **Current Federal Employees, Interns, and Detailees**
   ☒ Current Federal employees providing information in their capacity as federal employees (for example, PII collected using OPM, Treasury, or Fiscal Service forms related to employment with the federal government)
   a) ☒ Interns.
   b) ☒ Detailees.
   c) ☒ Other employment-related positions.

3. **Treasury Bureaus (including Departmental Offices)**
   ☒ Other Treasury Bureaus.

4. **Other Federal Agencies**
   ☒ Other federal agencies.

5. **State and Local Agencies**
   ☒ State and local agencies.

6. **Private Sector**
   ☒ Private sector organizations (for example, banks and financial organizations, data brokers or other commercial sources).

7. **Other Sources**
   ☐ Other sources not covered above (for example, foreign governments).

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

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

Section 3.3(a) 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.
   The Privacy Act Statement was provided to the individual:
   a) ☒ on the form in which the PII was collected
   b) ☐ on a separate sheet of paper that the individual could retain; or
   c) ☐ in an audio recording or verbally at the point where the information was collected (e.g., on the phone) or
   d) ☒ other: CAIA warning banner contains privacy information related to logging into ESM.

3. The Privacy Act Statement contains the following:
   a) ☒ The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
   b) ☒ Whether disclosure of such information is mandatory or voluntary.
   c) ☒ The principal purpose or purposes for which the information is intended to be used.
   d) ☒ The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
   e) ☒ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

Section 3.3(b) 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(c) Justification of Social Security Numbers & 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 approved Fiscal Service uses of SSNs apply:
   a) ☐ security background investigations;
   b) ☐ interfaces with external entities that require the SSN;
   c) ☐ a legal/statutory basis (e.g. where collection is expressly required by statute);
   d) ☐ when there is no reasonable, alternative means for meeting business requirements;
   e) ☐ statistical and other research purposes;
   f) ☒ delivery of government benefits, privileges, and services;
   g) ☐ for law enforcement and intelligence purposes;
   h) ☐ 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
   i) ☐ as a unique identifier for identity verification purposes.

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) ☐ 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: SSNs are only going to be used in the HR Service Delivery module. This module requires a HR related role on the platform to access any information in the HR module. There are other controls in the platform with the HRSD module to secure certain workflow like labor relations from other HR users. SSN would only be included on documents provided to HR in connection with an HR related service offered by HR. These documents would be attached to cases and assigned for work. The agent assigned would copy the documents provided into the system of record it is required for as the evidence required for that work item. The attachment would remain in the HR document management solution for 90 days after the case is closed in case there are questions about a particular case. Once the 90 mark is hit the attachments are deleted and the case would remain with the file name of the document provided without the ability to open it or retrieve it in ESM.

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

1. ☐ Not Applicable, 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

3. ☒ Full SSNs are collected, and the individual **will** be denied the benefit, or privilege provided by law if they refuse to disclose their SSN. Denial of this right, benefit or privilege does not violate the law because:

   ☒ SSN disclosure is required by Federal statute or Executive Order;

   OR

   ☐ The SSN is disclosed to a Federal, state, or local agency that maintains a system of records that was in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

Section 3.3(e) 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).

Although the Department of the Treasury may not keep records describing how any individual uses First Amendment rights, in certain instances records describing First Amendment rights may be maintained but only if the following conditions are met:

- The law specifically authorizes it. For instance, an individual's religious affiliation is made known when verifying contributions above a specified amount on tax returns or describing contributions to tax exempt groups of which he or she is a member.
- The individual expressly authorizes it. For example, the individual provides information regarding experience as a group leader in a political organization to demonstrate leadership skills when applying for a government position.
- The record is pertinent to and within the scope of an authorized law enforcement activity in which political or religious activities may be used as a cover for illegal activities.

1. ☒ Not Applicable. The system or project does **not** maintain information describing how individuals exercise their rights guaranteed by the First Amendment.

2. ☐ The system or project **does** maintain information describing how individuals exercise their rights guaranteed by the First Amendment. If you checked this box, please check the box below that explains Fiscal Service's authorization for collecting this information:
   a) ☐ The individual about whom the information was collected or maintained expressly authorized its collection/maintenance.
   b) ☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity.

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

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

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

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

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

1. ☒ **None** of the information maintained in the system or by the project that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act.

2. ☐ All ☐ Some of the PII maintained in the system or by the project is part of a system of records and **is** exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act

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).

4. ☐ **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).

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

1. ☒ **None** of the information maintained in the system or by the project that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act.

2. ☐ For all information maintained in the system or by the project that is part of a system of records that is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act, the following efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible without interfering with the (☐ law enforcement, ☐ intelligence, ☐ other) mission requirements for which the system or project was created:
   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 (☐ before ☐ after) the adverse determination is made.

e) ☐ Other:

3. ☐ No additional efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible because it would interfere with mission requirements.

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

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

1. ☒ The records maintained by this system or project are **not** used to make any adverse determinations about individuals.

2. ☐ The records maintained by this system or project are used to make adverse determinations about individuals and:
   A. ☐ These records were exempted from the Privacy Act provision that requires collection directly from the subject individual to the greatest extent practicable.
   B. ☐ These records were not exempted from the requirement to collect information directly from the individual to the greatest extent practicable and
      a) ☐ All records used to make an adverse determination are collected directly from the individual about whom the decision is made.
      c) ☐ 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.
      d) ☐ 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:
         1) ☐ alert the individual to the fact that their conduct is being observed or investigated;
         2) ☐ cause the individual to alter or modify their activities to avoid detection;
         3) ☐ create risks to witnesses or other third parties if the individual is alerted to the fact that their conduct is being observed or investigated;
         4) ☐ Other:

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

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

   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 (☐ are ☐ are not) exempt from the access provisions in the Privacy Act, 5 U.S.C. 552a(d).
   c) ☐ Individuals who provide their information directly to Fiscal Service 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 (☐ before ☐ after) it is used to make a final, adverse determination about them.
   d) ☐ Individuals who provide their information directly to Fiscal Service 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.
   e) ☐ 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).
   f) ☐ Other:

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).
   c) ☐ Technical and/or administrative controls 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.
   d) ☐ Address verification and correction software (software that validates, updates, and standardizes the postal addresses in a database).
   e) ☐ Other:

Section 4.2 Data Mining

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

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

1. ☒ The information maintained in this system or by this project **is not** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act. Therefore, no privacy or civil liberties issues were identified in responding to this question.

2. ☐ The information maintained in this system or by this project **is** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act. This system is included in Treasury's annual report to Congress which can be found on the external Treasury privacy website.

3. ☐ The information maintained in this system or by this project **is** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act, but this system is not included in Treasury's annual report to Congress which can be found on the external Treasury privacy website. This system will be added to the next Treasury Data-mining report to Congress.

Section 4.3 Computer Matching

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

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

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

Section 4.3(a) Records in the system used in a computer matching program

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.

Section 4.3(b) Is there a matching agreement?

1. ☒ Not Applicable

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.

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

1. ☒ Not Applicable

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.
   b. ☐ Before any information subject to the matching agreement is used to suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to an individual:
      i. ☐ The individual receives notice and an opportunity to contest the findings; **OR**
      ii. ☐ The Data Integrity Board approves the proposed action with respect to the financial assistance or payment in accordance with Section (p) of the Privacy Act before taking adverse action against the individual.

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

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

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

1. ☒ PII maintained in the system or by the project is **not** shared with agencies, organizations, or individuals external to Treasury except as authorized by the 12 exceptions in 5 USC Section 552(a)(b)(1) thru (b)(12) (disclosures allowed without first obtaining the consent of the individual, including publishing applicable routine uses in the appropriate systems of records notices).

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

Section 4.4(b) Accounting of Disclosures

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

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

Section 4.4(c) Making the Accounting of Disclosures Available

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 to agencies, organizations, or individuals external to Treasury.

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.

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 are not exempt from the requirement to make the accounting available to the individual named in the record. A log is **not** maintained regularly but is capable of being constructed in a reasonable amount of time upon request. The information necessary to reconstruct the log (i.e., date, nature, and purpose of each disclosure) is maintained for at least five years.

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

Records in a system of records subject to the Privacy Act may not be disclosed by "any means of communication to any person or to another agency" without the prior written request or consent of the individuals to whom the records pertain. 5 U.S.C. Sec. 552a(b). However, the Act also sets forth twelve exceptions to this general restriction. These 12 exceptions may be viewed at: https://www.justice.gov/usam/eousa-resource-manual-139-routine-uses-and-exemptions

Unless one of these 12 exceptions apply 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 allow agencies to include in a notice published in the Federal Register, a list of routine uses. Routines uses are disclosures outside the agency that are compatible with the purpose for which the records were collected.

Section 4.4(e) Obtaining Prior Written Consent

1. ☒ The records maintained in the system of records are only shared in a manner consistent with one of the 12 exceptions in the Privacy Act, including the routine uses published in the Federal Register.

2. ☐ If a situation arises where disclosure (written, oral, electronic, or mechanical) must be made to anyone outside of Treasury who is not listed in one of the 12 exceptions in the Privacy Act (including the published routine uses), the individual's prior written consent will be obtained where feasible and appropriate.

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 Fiscal Service 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. ☐ Not Applicable

2. ☒ The system or project maintains information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government).

2. ☒ The project or system involves a new collection of information in identifiable form for 10 or more persons from outside the federal government.

3. ☐ The project or system completed an Information Collection Request ("ICR") and received OMB approval.

4. ☒ The project or system did not complete an Information Collection Request ("ICR") and receive OMB approval because while the system maintains information from Federal contractors, no new collection of information is required because all data are acquired from an existing source within Treasury.

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).

2. ☒ The records used in the system or by the project are covered by a NARA approved Treasury bureau Specific Records Schedule (SRS).

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) or Acceptable to Use (ATU).

Section 5.3(a)

1. ☒ The system is a federal information system subject to FISMA requirements.

2. ☒ The system completed a SA&A and received an ATO or ATU.

3. ☐ This is a new system has not yet been authorized to operate.

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 Fiscal Service duties.

5. ☒ All Treasury/Fiscal Service 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/Fiscal Service 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.

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 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?

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? If checked:
   a) ☒ 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.
   b) ☐ The system or project is not in compliance with all Section 508 requirements.