**Privacy and Civil Liberties Impact Assessment**

# Enterprise Data Management (EDM) System

May 11, 2026

## Contact Point

So Yeon (Christie) Kim

## Reviewing Official

George Apetse
Bureau Privacy and Civil Liberties Officer
Departmental Offices
Department of the Treasury

## Section 1: Introduction

PCLIAs are required for all systems and projects that collect, maintain, or disseminate personally identifiable information (PII). The system owner completed this assessment pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget (OMB) Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before: (1) developing or procuring information technology (IT) systems or projects that collect, maintain or disseminate PII from or about members of the public, or (2) initiating a new collection of information that: (a) will be collected, maintained, or disseminated using IT; and (b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons (not including agencies, instrumentalities, or employees of the federal government).
It is the policy of the Department of the Treasury ("Treasury" or "Department") and its Bureaus to conduct a PCLIA when PII is maintained in a system or by a project. This PCLIA provides the following information regarding the system or project: (1) an overview of its purpose and functions; (2) a description of the information collected; (3) a description of the how information is maintained, used, and shared; and (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy.

## Section 2: Artificial Intelligence (AI)

Pursuant to the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence:

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

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

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

This PCLIA is being conducted on:

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

## Section 3: System Overview

### Section 3.1: System/Project Description and Purpose

The Enterprise Data Management (EDM) system is a comprehensive data warehouse application that provides integrated business reporting to support Treasury’s human resources (HR), financial, and other reporting requirements. It serves as a centralized platform for managing Treasury’s strategies and data assets by organizing data from disparate systems into a robust data warehouse. The EDM system integrates Treasury’s HR line-of-business systems to deliver a single source of high-quality reports, dashboards, and analytics to executives, managers, employees, and other agencies. In addition to its full integration with the HRConnect product suite, EDM offers complementary data support services to enhance decision-making across the enterprise.

The Treasury Common Services Center (TCSC) is conducting this updated PCLIA for the EDM system that was previously approved on January 7, 2022 to reflect current system operations, data sources, and privacy controls.

The primary purpose of the EDM system is to support Treasury's mission by providing integrated, enterprise-wide reporting, and analytics for human resources and financial management. EDM functions as a centralized data warehouse that consolidates data from authoritative source systems in order to produce standardized reports, dashboards, and analytics for Treasury executives, managers, and authorized users.

EDM receives data from source systems, processes data for reporting purposes, and presents aggregated or role-based views to authorized users.

The system is comprised of the following components:

- Data ingestion and integration services that receive data feeds from source systems;
- A Microsoft Structured Quert Language (SQL) Server-based data warehouse environment hosted on Azure Cloud services as Infrastructure as-a Service (IaaS);
- Reporting and analytics tools, including the Data Insight Portal, used to generate standard and ad hoc reports.

PII is stored within the EDM data warehouse environment as received from authoritative source systems. The EDM program collects/receives PII maintained in the system from the authoritative systems such as HRConnect, National Finance Center (NFC) Payroll, and the Treasury Information Executive Repository (TIER). The EDM program uses the information in the system to support enterprise reporting, workforce analytics, financial oversight, and compliance requirements. PII is used to generate standardized reports and dashboards and is not used to make automated decisions or take adverse actions against individuals.

**EDM Functions:**

Data from transaction systems is ingested into databases that make up the data warehouse. These databases are architected to provide data sources that deliver data for customers to support reporting compliance needs. A sophisticated data authorization scheme ensures that customers only view data that is specific to their role. A standard catalog of reports is established and maintained by the EDM team based on guidance from Data Stewards of the individual transaction data sets. These standard reports are available via browser access using comprehensive tools such as the Data Insight Portal. Data in EDM is managed in Microsoft SQL Server Commercial Off the Shelf (COTS) technology and the Treasury identity management services for customer authentication. The EDM platform supports reporting for the following primary business functions:

- **Workforce Analytics**

Workforce Analytics Reporting Service (WARS) is a standard catalog of reports for HR and payroll compliance reporting available to all HRConnect shared services customers via browser interface. WARS transforms core back-office business functions (e.g., moving HR functions from a processing-centric capability supported by Treasury and NFC legacy systems), to a

strategic-centric capability enabled through its commercial software. Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services, and processes (i.e., personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers and employees.

- **Treasury Finance applications**

Data from the TIER system is provided to the EDM data warehouse. The TIER system collects standard financial data monthly from Treasury bureau core financial systems. The EDM platform hosts reports and dashboards using Data Insight Portal – Treasury Financial Data Webapp (TFDW). The Data Insight Portal – TFDW is available only to Treasury Executives where the TIER reports and dashboards are accessed.

- **The U.S. Mint Sales Data**

Data from The U.S. Mint on sales of collectible coins that will be used to analyze and optimize revenue stream. These coins include American Silver Eagles, American Gold Eagles, commemorative coins, etc. The U.S. Mint's sales data will be migrated from their AWS Data Retention system into EDM's Azure Data Lake. All future sales data will be directly copied and integrated from the U.S. Mint vendor PFSWeb to the EDM Azure System, Data Lake. Data hosted in EDM Azure Data Lake will enable the U.S. Mint data scientists to perform data analytics and reporting. The sales data includes purchase order details, including PII, such as customers' names, and their addresses. PII identified fields is protected by EDM and accessible only to authorized U.S. Mint personnel.

EDM provides services Treasury-wide as well as to non-Treasury customers through the Treasury Shared Services Division.

The EDM program discloses the information in the system to the extent required by the Freedom of Information Act and as allowed by the Privacy Act of 1974 (including the routine uses in the applicable SORN: Treasury .001 - Treasury Payroll and Personnel System, Federal Register / 89 FR 25688 (Apr. 11, 2024); OPM/GOVT-1 - General Personnel Records - 77 FR 73694 (Dec. 11, 2012), and US Mint .009 - Order Management System - 79 FR 49376 – (Aug. 20, 2014) & Retail Sales System (RSS); Customer Mailing List; Order Processing Records for Coin Sets, Medals and Numismatic Items; Records of Undelivered Orders; and Product Descriptions, Availability and Inventory.

The EDM program identified the following privacy risks during collection, use, and disclosure:

1. Data Aggregation and Linkage Risk: The system aggregates data from multiple sources increasing the risk that combined datasets may reveal sensitive information or create detailed profiles beyond the original purpose of collection.

   **Mitigation**: EDM implements layered controls to mitigate data aggregation and linkage risk. Only required data elements are integrated for approved use cases. Access to aggregated datasets is restricted by using role-based access control (RBAC) and least privilege principles with separation of duties enforced for data engineering, analytics, and administrative functions.

2. Secondary Use: Information collected for one purpose may be used for unrelated purposes (e.g., analytics, profiling, or cross-agency use) without proper authorization or notice.
   **Mitigation**: EDM enforces strict use controls to mitigate the risk of secondary use of PII. All data use is governed by documented use cases and approved data-sharing agreements (e.g., ISA/MOU), ensuring information is used only for its intended purpose. Any new or expanded use of data requires formal review and approval through EDM change control board and data governance processes.
3. Insider Threat / Misuse of Access: Authorized users may intentionally or unintentionally access, use, or disclose information beyond their official duties.
   **Mitigation**: EDM implements layered access control to mitigate insider threat and misuse of access in accordance. Access to PII is strictly controlled using RBAC and least privilege principles, with periodic access reviews and provisioning/deprovisioning tied to user roles and job responsibilities.
4. Data Integrity and Accuracy Risk: Inaccurate, incomplete, or outdated data may result in adverse decisions or impacts to individuals, including financial or reputational harm.
   **Mitigation**: EDM implements data quality and integrity controls to mitigate risks associated with inaccurate, incomplete, or outdated PII. Data ingestion processes include automated validation, reconciliation, and error handling to ensure accuracy and completeness of data from source systems. Data is regularly refreshed and synchronized based on defined schedules and authoritative sources to maintain timeliness and consistency.
5. Over-Retention of Data: Retaining data longer than necessary increases the risk of exposure in the event of a breach and may violate records retention requirements.
   **Mitigation**: EDM enforces strict data retention to mitigate the risk of over-retention of PII. Data is retained only for the minimum period necessary to support authorized business functions and in compliance with Treasury records retention schedules and the National Archives and Records Administration requirements.
6. Improper Data Sharing or Disclosure: Information may be shared with other agencies or partners without proper authorization, agreements, or controls, leading to unauthorized disclosure.
   **Mitigation**: EDM enforces strict data sharing governance and technical controls to prevent improper sharing or unauthorized disclosure of PII. All data sharing with external agencies or partners requires formal authorization and documented agreements, such as Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU), which define permissible use, data elements, and security requirements.
7. Cloud and Third-Party Exposure Risk: Use of cloud services or contractors introduces the risk of data exposure due to misconfigurations, insufficient controls, or vendor access.
   **Mitigation**: EDM implements cloud security controls to mitigate the risk of data exposure in Azure. The Azure environment is configured using secure baselines and hardened configurations, with continuous configuration monitoring and vulnerability management to prevent misconfigurations. Access to cloud resources and PII is strictly controlled RBAC, least privilege, and multi-factor authentication.

8. Insufficient Audit and Monitoring: Lack of adequate logging and monitoring may delay detection of unauthorized access, misuse, or breaches.
   **Mitigation**: EDM implements audit logging and continuous monitoring controls to mitigate the risk of unauthorized access or misuse of PII. Audit logs are enabled across the Azure environment, including data access and query activity. Logs are centrally collected, protected, and retained to support analysis and forensic investigations.
9. Large-Scale Breach Impact: Due to centralized storage, a single incident could expose data affecting a large number of individuals, increasing harm and reporting obligations.
   **Mitigation**: EDM implements security architecture to mitigate the risk of large-scale breach impact associated with centralized PII storage. Sensitive data is protected encryption at rest and in transit using FIPS 140-2 compliant mechanisms, and access is strictly controlled through RBAC, least privilege, and multi-factor authentication. Data is segmented across secure environments based on data domain and data zone (e.g., raw, curated, analytics) and to limit the scope of exposure in the event of a compromise.
10. Transparency and Notice Gaps: Privacy documentation (e.g., SORN, PCLIA) may become outdated or incomplete, reducing transparency about how data is collected, used, and shared.
    **Mitigation**: EDM implements formal privacy governance and documentation management processes to mitigate the risk of outdated or incomplete transparency. Privacy documentation (e.g., SORN, PCLIA) is maintained and regularly reviewed to ensure accuracy and completeness.

## Section 3.2: Authority to Collect

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

- *Homeland Security Presidential Directive 12 (HSPD-12)*
- *Treasury Directive 80-05, Records and Information Management Program*
- *5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and*
- *Executive Orders 9397, as amended by 13478, 9830, and 12107.*

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

- *31 U.S.C. 321 – General authorities of the Secretary establish the mission of the Department of the Treasury*
- *5 U.S.C. 301 – Department regulations for the operations of the department, conduct of employees, distribution and performance of its business, the custody, use, and preservation of its records, papers, and property.*

## Section 3.3: Privacy Act Applicability; SORN Requirement

Under certain circumstances, federal agencies are allowed to exempt a system of records from certain provisions in the Privacy Act. This means that, with respect to information systems and papers files that maintain records in that system of records, the agency will not be required to comply with the requirements in Privacy Act provisions that are properly exempted. If this system or project contains

records covered by the Privacy Act, the applicable Privacy Act system of records notice(s) (SORNs) (there may be more than one) that cover the records in this system or project must list the exemptions claimed for the system of records (it will typically say: "*Exemptions Claimed for the System*" or words to that effect).

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

**Section 3.3(a) Please check ALL statements below that apply to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.**

1. ☐ The system or project does not retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. A SORN is not required with respect to the records in this system.
2. ☒ The system or project does retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. A SORN is required with respect to the records in this system.
3. ☐ A SORN was identified in the original PCLIA and a determination was made during this current PCLIA update that modifications [choose one] ☐ were ☐ were not required to that SORN. [If modifications were made, generally describe them here]. The current applicable SORN is: [Provide here the SORN number(s), system of records name(s) and the citation to the SORN(s) in the Federal Register.]
4. ☐ A SORN(s) was not identified or required in the original PCLIA, but a determination was made during this current PCLIA update that a SORN(s) is now required. The applicable SORN(s) is:[Provide here the SORN number(s), system of records name(s) and the citation to the SORN(s) in the Federal Register].
5. ☒ A SORN was published and no exemptions are taken from any Privacy Act requirements.
   ☐ Exemptions are claimed from the following Privacy Act provisions in the applicable SORN(s): [List here all exemptions taken in the applicable SORN; Hint: it's at the end of the SORN]: The citation to the applicable Notice of Proposed Rulemaking and/or Final Rule is[provide here the Federal Register Citation to the NPRM and Final Rule (if a Final Rule was required)].

## Section 4: Information Collection

### Section 4.1: Relevant and Necessary

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

**Section 4.1(a) Exemption Claimed from this Requirement?** ☒ The PII maintained in this system or by this project is ***not*** exempt from 5 U.S.C. § 552a(e)(1), the Privacy Act's requirement that an agency "*maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.*"

2. ☐ The PII maintained in this system or by this project ***is*** exempt from 5 U.S.C. § 552a(e)(1), because *[See the applicable SORN]*.

**Section 4.1(b) Continuously Assessing Relevance and Necessity** ☐ The PII in the system is not maintained in a system of records. Therefore, the Privacy requirements do not apply. *[Explain **here** what you do to ensure relevance and necessity despite the fact that the Privacy Act does not apply].*

2. ☐ The PII in the system is maintained in a system of records, but the agency exempted these records from the relevance and necessity requirement. *[Explain **here** what you do to ensure relevance and necessity to the extent possible despite the fact the records are exempt from this requirement].*
3. ☒ The system owner conducted an assessment prior to collecting PII for use in the system or project to determine which PII data elements and types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements. During this analysis, *in* conducting the "relevance and necessity" analysis that is documented in this PCLIA, the system owner reevaluated the necessity and relevance of all PII data elements and determined that they are still relevant and necessary. Every time this PCLIA is updated, this ongoing assessment will be revisited. If it is determined at any time that certain PII data elements are no longer relevant or necessary, the system owner will update this PCLIA to discuss how the data element was removed from the system and is no longer collected.
4. ☒ With respect to PII ***currently*** maintained (as of the time this PCLIA is being done) in the system or by the project, the PII *[choose one]* ☒ is ☐ is not limited to only that which is relevant and necessary to meet the system's or project's mission requirements. During the PCLIA process, the system always undergoes a review to ensure the continuing relevance and necessity of the PII in the system.
5. ☒ With respect to PII maintained in the system or by the project, there [choose one] ☒ is ☐ is not a process in place to continuously reevaluate and ensure that the PII remains relevant and necessary. During the PCLIA process, the system always undergoes a

review to ensure the continuing relevance and necessity of the PII on the system. If a determination is made that particular PII is no longer relevant and necessary in between PCLIA updates, this PCLIA will be updated at that time.

## Section 4.2: PII and/or information types or groupings

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

### Biographical/general information

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

### Other information

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

### Identifying numbers assigned to individuals

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

### Specific Information/File Types

| | | |
|---|---|---|
| ☐ Taxpayer Information/Tax Return Information | ☐ Law Enforcement Information | ☒ Security Clearance/Background Check Information |
| ☐ Civil/Criminal History Information/Police Records (obtained from government source) | ☐ Civil/Criminal History Information/Police Records (obtained from commercial source) | ☐ Credit History Information (government source) |
| ☐ Protected Information (as defined in Treasury Directive 25-10) | ☐ Credit History Information (commercial source) | ☐ Bank Secrecy Act Information |

☐ Information provided under a confidentiality agreement
☐ Case files
☒ Personnel Files
☐ Business Financial Information (including loan information)
☐ Personal Financial Information (e.g., loan information)
☐ Information subject to the terms of an international or other agreement
☐ Passport information (state which passport data elements are collected if not all)
☐ Other: (please describe)

## Audit Log and Security Monitoring Information

☒ User ID assigned to or generated by a user of Treasury IT
☐ Files and folders accessed by a user of Treasury IT
☐ Biometric information used to access Treasury facilities or IT
☐ Passwords generated by or assigned to a user of Treasury IT
☐ Internet or other queries run by a user of Treasury IT
☐ Contents of files accessed by a user of Treasury IT
☐ Files accessed by a user of Treasury IT (e.g., web navigation habits)
☐ Date and time an individual accesses a facility, system, or other IT
☐ Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT.
☐ Public Key Information (PKI).
☐ Still photos of individuals derived from security cameras.
☐ Purchasing habits or preferences
☐ Internet Protocol (IP) Address
☐ Video of individuals derived from security cameras
☐ Commercially obtained internet navigation/purchasing habits of individuals
☐ Global Positioning System (GPS)/Location Data
☐ Secure Digital (SD) Card or Other Data stored on a card or other technology
☐ Device settings or preferences (e.g., security level, sharing options, ringtones).
☐ Network communications data
☐ Cell tower records (e.g., logs. user location, time etc.)
☐ Other: (please describe)

## Medical/Emergency Information Regarding Individuals

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

## Biometrics/Distinguishing Features/Characteristics of Individuals

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

## Identifying numbers for sole proprietors (including business information).

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

## 4.3 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 (only check if relevant to the purpose for collecting and using the information):

☐ Members of the general public (current association with the federal government, if any, is irrelevant to the collection and use of the information by the system or project).

☒ Retired federal employees.

*PII is stored within the EDM data warehouse environment as received from authoritative source systems to support enterprise reporting, workforce analytics, financial oversight, and compliance requirements. PII is used to generate standardized reports and dashboards for executive use.*

☒ Former Treasury employees.

*PII is stored within the EDM data warehouse environment as received from authoritative source systems to support enterprise reporting, workforce analytics, financial oversight, and compliance requirements. PII is used to generate standardized reports and dashboards for executive use.*

☒ Federal contractors, grantees, interns, detailees etc.

*PII is stored within the EDM data warehouse environment as received from authoritative source systems to support enterprise reporting, workforce analytics, financial oversight, and compliance requirements. PII is used to generate standardized reports and dashboards for executive use.*

☒ Federal job applicants.

*PII is stored within the EDM data warehouse environment as received from authoritative source systems to support enterprise reporting, workforce analytics, financial oversight, and compliance requirements. PII is used to generate standardized reports and dashboards for executive use.*

☐ Other: [Explain ***here***]. Discuss here how/why PII is collected from this source.

### 2. *Current Federal Employees, Interns, and Detailees*

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

☒ Interns.

☒ Detailees.

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

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

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

4. ***Other Federal Agencies***

***☐ Other federal agencies: (name each agency here and explain how/why PII is collected from this source.).***

5. ***State and Local Agencies***

☐ State and local agencies: (Name the State and local agencies here and explain how/why PII is collected from this source).

6. ***Private Sector***

☐ Private sector organizations (for example, banks and financial organizations, data brokers or other commercial sources): (Name the State and local agencies here and explain how/why PII is collected from this source.).

7. ***Other Sources***

☐ Other sources not covered above (for example, foreign governments).
(Name the other sources here and explain how/why PII is collected from this source).

## Section 4.3: Privacy and/or civil liberties risks related to collection

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

## Section 4.3(a) Collection Directly from the Individual to whom the PII pertains.

1. ☐ None of the PII in the system was collected directly from an individual to whom it pertains. . *[Explain if the third-party/agency from which you obtained the PII actually collected the PII directly from the individuals about whom it pertains. Be prepared to discuss below how you ensure the information received from the third-party is still accurate, complete and timely for the purposes for which you will use it)].* [Explanation here.]

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

### Section 4.3(b) Privacy Act Statements

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

### Section 4.3(c) Use of Full Social Security Numbers

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

### Section 4.3(d) Justification of Social Security Numbers

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

    ☐ security background investigations;

☒ interfaces with external entities that require the SSN; *(SSN is a required field for Payroll – that is a requirement of the payroll provider – NFC. There is no alternate employee identifier in the payroll system)*.

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

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

☐ statistical and other research purposes;

☐ delivery of government benefits, privileges, and services;

☐ for law enforcement and intelligence purposes;

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

☐ as a unique identifier for identity verification purposes.

## Section 4.3(e) Controls implemented to limit access to and or improper disclosure of full Social Security Numbers.

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

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

1. ☐ SSNs are maintained in *EDM. EDM does not directly collect SSNs. However, it maintains SSNs that are obtained from other systems or programs which have previously collected them from the individual*.
2. ☐ Full SSNs are collected, but no individual will be denied any right, benefit, or privilege provided by law if the individual refuses to disclose their SSN for use in the system or project. If the individual chooses not to provide their SSN *[please describe **here** what will happen (something less than denial of a privilege etc.) if the individual chooses not to provide their SSN].*
3. ☐ Full SSNs are collected, and the individual will be denied the following right, benefit, or privilege provided by law if they refuse to disclose their SSN: *Providing the SSN is voluntary. However, if the individual refuses to disclose their SSN, their application for Federal government position and benefits cannot be processed. Denial of this right, benefit or privilege does not violate the law because:*
4. [choose one of the two boxes below]:
    a. ☐ SSN disclosure is required by the following Federal statute or Executive Order: ;**OR**
    b. ☐ The SSN is disclosed to a Federal, state, or local agency that maintains a system of records that was in existence and operating before January 1,1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

### Section 4.3(g) Records describing how individuals exercise First Amendment rights

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

1. ☒ N/A. The system or project does ***not*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment.
2. ☐ The system or project ***does*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment. *If you checked this box, please check the box below that explains Treasury's authorization for collecting this information:*
    a. ☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance. The individual about whom the information was collected or maintained expressly authorized its collection by *[explain here how the individual expressly authorizes collection] (for example, individuals may expressly authorize collection by requesting in writing that Treasury share information with a third party, e.g., their Congressman];*
    b. ☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity because [generally discuss here the nature and purpose of the information collected and the law enforcement activity];

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

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

### Section 5.1: Ensuring accuracy, completeness, and timeliness of collected information, maintained, and shared when it is used to make determinations about individuals

The Privacy Act and Treasury policy require that Treasury bureaus and offices take additional care when collecting and maintaining information about individuals when it will be used to make determinations about those individuals (e.g., whether they will receive a federal benefit). This includes collecting information directly from the individual where practicable and ensuring that the information is accurate, relevant, timely and complete to assure fairness to the individual when making a determination about them. This section addresses the controls/protections put in place to address these issues.
The Privacy Act requires that Federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C § 552a(e)(5). If a particular system of records meets certain requirements (including the NPRM process defined in Section 3.1 above), an agency may exempt the system of records (or a portion of the records) from this requirement. Exemptions may be found at the bottom of the relevant SORN next to the heading: "*Exemptions Claimed for this System.*"

### Section 5.1(a). Exemption from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act

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

### Section 5.1(b) Protections in place despite exemption from the accuracy, relevance, timeliness, and completeness requirements

1. ☒ ***None*** of the information maintained in the system or by the project that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act.
2. ☐ For all information maintained in the system or by the project that is part of a system of records that is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act, the following efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible without interfering with the (*check one*) ☐ law enforcement ☐ intelligence ☐ other [*describe* ***here***] mission requirements for which the system or project was created [*choose* ***ALL*** *that apply*]:
    a. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals.
    b. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals without additional research and investigation to ensure accuracy, relevance, timeliness, and completeness.
    c. ☐ Individuals and organizations to whom PII from the system or project is disclosed (as authorized by the Privacy Act) determine its accuracy, relevance, timeliness, and completeness in a manner reasonable for their purposes before they use it to make adverse determinations about individuals.
    d. ☐ Individuals about whom adverse determinations are made using PII from this system or project are given an opportunity to explain or modify their information (*check one*) ☐ before ☐ after the adverse determination is made. During this process, individuals are allowed to: [*discuss* ***here***
    e. ☐ Other: (*please describe*):

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

### Section 5.1(c) Collecting information directly from the individual when using it to make adverse determinations about them.

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

1. ☒ The records maintained by this system or project are **not** used to make any adverse determinations about individuals☐ The records maintained by this system or project **are** used to make adverse determinations about individuals ***and*** *[check all that apply]:*

    a. ☐ These records ***were*** exempted from the Privacy Act provision that requires collection directly from the subject individual to the greatest extent practicable. Exemption of these records is proper because *[explain here why the records were exempted; See the applicable SORN].*
    b. ☐ These records were ***not*** exempted from the requirement to collect information directly from the individual to the greatest extent practicable ***and*** [*check the relevant box below and provide the information requested*].
        *i.* ☐ ***All*** records used to make an adverse determination are collected directly from the individual about whom the decision is made. ☐ 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].*

iii. ☐ ***None*** of the records used to make adverse determinations are collected directly from the individual about whom determinations are made because seeking the information directly from the individual might *[select **ALL** that apply]:*

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

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

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

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

**Section 5.1(d) Additional controls designed to ensure accuracy, completeness, timeliness, and fairness to individuals in making adverse determinations**

1. **Administrative Controls**. Individuals about whom information is collected are given the following opportunities to amend/correct/update their information to ensure it is accurate, timely and complete to the extent reasonably necessary to assure fairness when it is used to make a determination about them: ☒ The PII collected for use in the system or project is NOT used to make adverse determinations about an individual's rights, benefits, and privileges under federal programs.

b. ☐ The records maintained in the system or by the project are used to make adverse determinations and (*select one*) ☐ are ☐ are not exempt from the access provisions in the Privacy Act, 5 U.S.C. 552a(d).

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

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

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

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

g. ☐ Other: [please describe here].

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

b. ☒ Automated data feeds are used to refresh/update the information in the system (where the system is reliant on updates from another system). These automated data feeds occur: *on schedules determined by the source transaction systems that provide data to EDM (i.e. HRConnect, NFC Payroll) and updates are made to the EDM system based on logic specified by the source transaction system*.

c. ☒ Technical and/or administrative controls are put 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: *performing data validation of employee records to ensure all separate source records match the master HRConnect record for the employee.*

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

e. ☐ Other: [please describe here]

## Section 5.2 Data-Mining

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

## Section 5.2(a) Is the PII maintained in the system used to conduct data-mining?

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

## Section 5.3 Computer Matching

The Computer Matching and Privacy Protection Act (CMPPA) of 1988 amended the Privacy Act by imposing additional requirements when Privacy Act systems of records are used in computer matching programs.
Pursuant to the CMPPA, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated systems of records or a system of records with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8). Matching programs must be conducted pursuant to a matching agreement between the source (the agency providing the records) and recipient agency (the agency that receives and uses the records to make determinations). The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

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

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

### Section 5.3(b) Is there a matching agreement?

1. ☒ N/A
2. ☐ There is a matching agreement in place that contains the information required by Section (o) of the Privacy Act.
3. ☐ There is a matching agreement in place, but it does not contain all of the information required by Section (o) of the Privacy Act. The following actions are underway to amend the agreement to ensure that it is compliant. [discuss **here** the issues that were discovered that required amendment and how those issues are being mitigated/fixed]: Discuss here.

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

1. ☒ N/A
2. ☐ The bureau or office that owns the system or project conducted an assessment regarding the accuracy of the records that are used in the matching program and the following additional protections were put in place:

a. ☐ The results of that assessment were independently verified by [*explain how and by whom accuracy is independently verified; include the general activities involved in the verification process*].
b. ☐ Before any information subject to the matching agreement is used to suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to an individual:
   i. ☐ The individual receives notice and an opportunity to contest the findings; **OR**
   ii. ☐ The Data Integrity Board approves the proposed action with respect to the financial assistance or payment in accordance with Section (p) of the Privacy Act before taking adverse action against the individual.

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

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

### Section 5.4(a) PII shared with/disclosed to agencies, organizations or individuals outside Treasury

1. ☐ PII maintained in the system or by the project is ***not*** shared with agencies, organizations, or individuals external to Treasury.
2. ☐ PII maintained in the system or by the project ***is*** shared with the following agencies, organizations, or individuals external to Treasury:
3. ☒ All external disclosures ***are*** authorized by the Privacy Act (including routine uses in the applicable SORN).

### Section 5.4(b) Accounting of Disclosures

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

### Section 5.4(c) Making the Accounting of Disclosures Available

1. ☐ The records are not maintained in a system of records subject to the Privacy Act so an accounting is ***not*** required.
2. ☐ No external disclosures are made from the system.
3. ☐ The Privacy Act system of records maintained in the system or by the project ***is*** exempt from the requirement to make the accounting available to the individual named in the record. Exemption from this requirement was claimed because: [please state here why the records in this system of records were exempted from this requirement].
4. ☐ The Privacy Act system of records maintained in the system or by the project is ***not*** exempt from the requirement to make the accounting available to the individual named in the record and a log is maintained regularly. The log is maintained for at least five years and includes the date, nature, and purpose of

each disclosure (not including intra-agency disclosures and FOIA disclosures) of a record to any person or to another agency (outside of Treasury) and the name and address of the person or agency to whom the disclosure is made.

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

### Section 5.4(d) Obtaining Consent Prior to New Disclosures Not Authorized by the Privacy Act

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

### Section 5.4(e) Obtaining Prior Written Consent

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

## Section 6: Compliance with Federal information management requirements

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

### Section 6.1: The Paperwork Reduction Act

The PRA requires OMB approval before a Federal agency may collect standardized data from 10 or more respondents within a 12-month period. OMB also requires agencies to conduct a PIA (a Treasury

PCLIA) when initiating, consistent with the PRA, a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

### Section 6.1(a)

1. ☐ The system or project maintains information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government)
2. ☒ The project or system involves a new collection of information in identifiable form for *10 or more people 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 *information in EDM is coming from other systems that already completed an ICR.*

### Section 6.2: Records Management - NARA/Federal Records Act Requirements

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

**Section 6.2(a)** ☒ The records used in the system or by the project are covered by a NARA's General Records Schedule (GRS). *The GRS is 2.2 Item 010, Employee Management Administrative Records*.

2. ☐ The records used in the system or by the project are covered by a NARA approved Treasury bureau Specific Records Schedule (SRS). The SRS *[please provide here the specific schedule name and identifying number]*
3. ☐ On [*please state the date on which NARA approval was sought*] the system owner sought approval from NARA for an SRS and is awaiting a response from NARA. *[State here the retention periods you proposed to NARA]*.
4. ☐ The system owner is still in the process of developing a new records schedule to submit to NARA.

### Section 6.3: E-Government Act/NIST Compliance

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

**Section 6.3(a)** ☒ The system is a federal information system subject to FISMA requirements.

2. ☒The system last completed an SA&A and received an ATO on: 03/28/2024 .
3. ☐This is a new system has not yet been authorized to operate. The expected to date for receiving ATO is *[please state here the expected date on which you expect authorization will be granted].*

4. ☒The system or project maintains access controls to ensure that access to PII maintained is limited to individuals who have a need to know the information in order to perform their official Treasury duties.
5. ☒ All Treasury/bureau security requirements are met when disclosing and transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury system or project to internal or external parties.
6. ☒ This system or project maintains an audit log of system users to ensure they do not violate the system and/or Treasury/bureau rules of behavior.
7. ☐ This system or project has the capability to identify, locate, and monitor individuals or groups of people other than the monitoring of system users to ensure that they do not violate the system's rules of behavior. *[If checked, please describe this capability here, including safeguards put in place to ensure the protection of privacy and civil liberties.]*

### Section 6.4: Section 508 of the Rehabilitation Act of 1973

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

### Section 6.4(a)

1. ☐ The project or system will ***not*** involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)?
2. ☒ The project or system ***will*** involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)? *If checked:*
3. ☒ The system or project complies with all Section 508 requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities.
4. ☐ The system or project is not in compliance with all Section 508 requirements. The following actions are in progress to ensure compliance: [please describe here the efforts underway to ensure compliance*]*.

## Responsible Officials Certification

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

☐ This system was reviewed pursuant to continuous monitoring requirements. Since the PCLIA was last updated, significant changes have been made to the system that warranted

modifications to the PCLIA. I have reviewed all responses in the PCLIA, and it reflects the current, accurate, and complete status of the system, including the significant changes.

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

So Yeon (Christie) Kim (System Owner and Program Manager)

## Approval Signature

_____

Ryan Law
Deputy Assistant Secretary
Privacy, Transparency and Records
Department of the Treasury