Privacy and Civil Liberties Impact Assessment

for the

HRConnect System

October 28, 2024

Nicolaos Totten

Reviewing Official

Timothy H. Skinner, JD
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 Office of the Chief Information Officer (OCIO) Enterprise Applications that owns the system, is conducting this PCLIA for HRConnect. The program is updating a previous PCLIA for this system that was approved on December 16, 2021 to:

a. Remove vaccination status information: Per Executive Order No. 14043, HRConnect collected and stored vaccination status for Federal civilian employees. The PCLIA on collection of vaccination status was approved on February 22, 2021. However, on May 9, 2023, President Biden signed an Executive Order (EO) revoking EO 14043, which had required vaccination for Federal civilian employees. Effective May 12, 2023, all prior guidance from the Safer Federal Workforce Task Force ("Task Force") implementing the requirements of Executive Order No. 14043 has also been revoked. In accordance with this Executive Order, HRConnect does not collect any new information regarding vaccination status of employees (i.e., no new vaccination data has been collected since before May 9,

2023) nor is vaccination status information available to managers or personnel specialists in HRConnect. HRConnect will remove the previously collected data in compliance to the NARA standards outlined in GRS 2.7 as of September 30, 2024.

b. Allow employees to submit the Office of Government Ethics (OGE) Form 450 electronically: As part of continuous enhancement of HRConnect, the system will allow employees to submit the OGE Form 450 electronically starting September 30, 2024. As for the financial information, managers who have need to know will be able to see the content of the information in order to approve forms for employees who report to them.

The main purpose of HRConnect is to help Treasury meet its mission by providing an online personnel system for managers, supervisors, employees, and human resource specialists to input and process personnel and payroll data on Treasury (and non-Treasury) federal government employees. The objective of HRConnect as a personnel system is to provide an intuitive platform for the various groups of users to ensure all employee personnel information within HRConnect is current, valid, and accurate to ensure success payment of employees. HRConnect allows Enterprise Applications to support the human resources functions as part of a cross-services initiative to reduce federal government expenditures. The following are the non-Treasury HRConnect users (or components of those users):

#	Non-Treasury, HRConnect Users
1	Department of Agriculture, Office of the Chief Information Officer – CTS (Client Technology Services)
2	U. S. Agency for International Development (USAID)
3	Architectural and Transportation Barriers Compliance Board (US Access Board)
4	Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE)
5	Department of Labor (DOL)
6	Denali Commission
7	Federal Reserve, Bureau of Consumer Financial Protection (CFPB)
8	Gulf Coast Ecosystem Restoration Council (GCERC)
9	Office of Government Ethics (OGE)
10	Federal Housing Finance Agency Office of Inspector General (FHFA OIG)
11	Department of Homeland Security, U.S. Secret Service (USSS)
12	Department of Housing and Urban Development (HUD)
13	Department of Housing and Urban Development, Office Inspector General (HUD OIG)
14	Government Accountability Office (GAO)
15	United States Congress, Commission on Security and Cooperation in Europe (CSCE)
16	Armed Services Retirement Home (AFRH)
17	Federal Mine Safety and Health, Fed Mine Safety Health Rev Com
18	Commission on People's Republic of China (CECPRC)
19	Veterans Affairs Office of Inspector General (VA OIG)
20	Department of Commerce: 1) Office of the Secretary (OS) 2) Economic Development Administration (EDA) 3) Bureau of Economic Analysis (BEA) 9) National Telecommunications and Information Administration (NTIA) 10) National Technical Information Service (NTIS) 11) Bureau of the Census

#	Non-Treasury, HRConnect Users	
	4) National Oceanic and Atmospheric Administration (NOAA) 5) International Trade Administration (ITA) 6) U. S. Patent and Trademark Office (USPTO) 7) National Institute of Standards and Technology (NIST) 8) Minority Business Development Agency (MBDA)	12) Office of the Inspector General (OIG) 13) Bureau of Industry and Security (BIS)

HRConnect consists of a general support system (GSS) and a major application (MA) also known as Platform as a Service or Software as a Service; customized PeopleSoft Human Capital Management (HCM) software residing on the Oracle Cloud Infrastructure's GovCloud Infrastructure as a Service Cloud Service Provider. HRConnect collects and maintains PII elements listed in Section 4.2 which are extracted from forms required as part of the hiring/onboarding and employee management processes (e.g., personnel, payroll, retirement, benefits, etc.). HRConnect also collects information in compliance with the Office of Personnel Management (OPM) and the Office of Management and Budget (OMB) reporting requirements.

The OCIO Enterprise Applications collects/receives PII maintained in the system from:

1. Applicants who receive and accept job offers for employment with a federal agency that is serviced by HRConnect. These individuals submit the information in Section 4.2 into the OPM USA Staffing system using the forms listed in Appendix A. These forms are required to complete the hiring and onboarding process. For those agencies that use USA Staffing, these forms are completed within USA Staffing and some of the information in these forms (not the form itself) and in USA Staffing are sent to HRConnect through a secure New Hire Interconnection (NHI) Application Programming Interface (API). Under the Paperwork Reduction Act (PRA), HRConnect collects information using the forms listed in Section 4.2. All information that is collected in HRConnect using forms subject to the PRA have been approved by the OMB Director and Treasury processes and, therefore, been assessed and determined to be relevant and necessary. For agencies who do not use the New Hire Interconnection, new employees submit forms containing PII electronically to Human Resource Specialists to input directly and manually into HRConnect.
2. The second type of individuals who provide PII are existing employees. Existing employees that are employed in an agency that uses Treasury's HRConnect system provide PII to update their personal information (e.g., address, contact information, etc.)
3. Human Resources personnel specialists who enter information on behalf of existing employees into HRConnect.
5. The National Finance Center (NFC), Treasury's payroll provider, provides plain text files, containing PII that are loaded into the HRConnect system. These flat files are loaded daily into HRConnect and contain employee PII.

The information collected and maintained in the system is used by Treasury and non-Treasury HRConnect users to record personnel data, performance, and administrative transactions for Human Resource purposes. Additionally, recruiting information is collected and maintained in the system to track progress for filling, and later managing the lifecycle of the position.

The OCIO Enterprise Applications 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 - 89 FR 25688 (Apr. 11, 2024)).

The OCIO Enterprise Applications identified the following privacy risks during collection, use, and disclosure: If unauthorized access to HRConnect occurs, systematically or through an individual misusing information, PII may be disclosed to unintended recipients internal and/or external to Treasury. Individuals whose PII is unintentionally disclosed may be subjected to personal harm or identify theft. Additionally, PII exposure could negatively impact Treasury since it is the responsibility of Enterprise Applications (EntApps) to protect the information.

The OCIO Enterprise Applications has taken the following steps/implemented the following controls to protect the PII in the system during collection, use, and disclosure:

> Access to the data by a user is determined based upon the roles assigned to the user's profile. Roles are assigned based on position. Specifically, users will only have access to the data that is inherently theirs, such as their own PII, or required to meet the requirements of their position. In the case of managers, they will have access to their own PII as well as limited information of those employees assigned to them. Additional roles may be assigned using strict 'need-to-know' criteria. The criteria, procedures, controls, and responsibilities regarding access are documented and audited periodically. Users must access the HRConnect URL address via a secure and recognized connection to the Treasury network gateway and authenticate to the application using multi factor authentication via a PIV card, Login.gov or ID.me. The data in the system is shared with data owners (both internal and external to Treasury). Authorized third parties receive extracts of data in the system on a 'need-to-know' basis and in accordance with a written agreement between themselves and the U.S. Department of Treasury, Office of the Chief Information Office, Enterprise Applications (EntApps), and the HR Line of Business, HRConnect Program Office. The agencies must then adhere to the prescribed configuration management principles and procedures in conjunction with the Enterprise Application Cybersecurity (EAC) information systems protocols to set up a periodic file feed with the extracted information. In support of the HSPD-12 Initiative, HRConnect implemented an application programming interface (API) platform to provide data exchange services.

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 *HRConnect* to collect information:

1. Homeland Security Presidential Directive 12 (HSPD-12)
2. Treasury Directive 80-05, Records and Information Management Program
3. General Duty Clause, Section 5(a)(1) of the Occupational Safety and Health (OSH) Act of 1970, Executive Order 12196, Occupational safety and health programs for Federal employees (Feb. 26, 1980), OMB Memorandum M-20-23, Aligning Federal Agency Operations with the National Guidelines for Opening Up America Again (Apr. 20, 2020), and 5 U.S.C. § 6329c(b)

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. *Treasury .001- Treasury Payroll and Personnel System - 89 FR 25688 (Apr. 11, 2024).*

6. ☐ 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? 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 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 Appendix B for a list of acceptable bases for claiming this exemption and cut and paste **here** all that apply]*.

Section 4.1(b) Continuously Assessing Relevance and Necessity. Helpful Hint: Unless you check Box 1 or Box 2 below, you must check, if true, Boxes 3-5 (all are required by OMB). Also, please provide the required information. If not true, you must explain in the space provided why these reviews did not happen.

1. ☐ The PII in the system is not maintained in a system of records. Therefore, the Privacy requirements do not apply. *[Explain **here** what you do to ensure relevance and necessity despite the fact that the Privacy Act does not apply]*.
2. ☐ The PII in the system is maintained in a system of records, but the agency exempted these records from the relevance and necessity requirement. *[Explain **here** what you do to ensure relevance and necessity to the extent possible despite the fact the records are exempt from this requirement]*.
3. ☒ The system owner conducted an assessment prior to collecting PII for use in the system or project to determine which PII data elements and types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements. During this analysis*, in* conducting the "relevance and necessity" analysis that is documented in this PCLIA, the system owner reevaluated the necessity and relevance of all PII data elements and determined that they are still relevant and necessary. Every time this PCLIA is updated, this ongoing assessment will be revisited. If it is determined at any time that certain PII data elements are no longer relevant or necessary, the system owner will update this PCLIA to discuss how the data element was removed from the system and is no longer collected.
4. ☒ With respect to PII ***currently*** maintained (as of the time this PCLIA is being done) in the system or by the project, the PII ☒ 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. 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 (legal and preferred)
☒ Age
☒ Date of birth
☒ Home physical/postal mailing address
☒ Zip Code
☒ Personal home phone, cell phone, or fax number

☒ Nationality
☒ Citizenship
☒ Ethnicity
☒ Gender
☒ Race
☒ Personal e-mail address

☐ Other: (please describe)

☒ Country of Birth
☐ Immigration Status
☒ Alias (including nickname)
☒ City or County of Birth
☒ Military Service Information
☒ Country or city of residence

Other information

☐ Resume or curriculum vitae
☒ Religion/Religious Preference
☐ Professional/personal references or other information about an individual's friends, associates or acquaintances.
☐ Sexual Orientation
☒ Group/Organization Membership

☒ Cubical or office number
☒ Education Information [please describe] Highest level of education, year graduated, school attended and major course of study
☒ Contact lists and directories (known to contain at least some personal information).
☒ Marital Status
☒ Information about children

☒ Veteran's preference
☒ Spouse Information
☒ Retirement eligibility information
☒ Information about other relatives.
☒ Other: Employment type (full or part-time), Eligibility for and coverage under Federal Employees Group Life Insurance Program (FEGLI), Eligibility for and coverage under Federal Employee Retirement System (FERS) coverage, Participation and and coverage under Federal Employee Health Benefits (FEHB) coverage, Child Care/Alimony, Deductions due to Indebtedness (Garnishments), Thrift Savings Program participation, Occupational series, Official Title Code, pay band, Whether the employee's position is temporary or permanent, Official title associated with the position, Work schedule type, Position Target Grade, Instant Message ID (IM) (table is under personal data CWR), Language proficiency (languages spoken

Identifying numbers assigned to individuals

☒ Full Social Security number
☒ Truncated Social Security Number (e.g., last 4 digits)
☒ Employee Identification Number
☐ Taxpayer Identification Number
☐ File/Case ID Number
☐ Alien Registration Number

☒ Personal device identifiers or serial numbers
☐ Internet Protocol (IP) Address
☒ Personal Bank Account Number
☐ Health Plan Beneficiary Number
☐ Credit Card Number
☐ Patient ID Number

☐ Vehicle Identification Number
☐ Driver's License Number
☐ License Plate Number
☒ Professional License Number
☐ Passport Number and information (nationality, date and place of issuance, and expiration date)
☒ Other: Number randomly assigned to personnel files and maintained by Office

of Human Resources (OHR) and provided to external vendors and internally within Treasury as a unique identifier to allow the development of aggregate/ statistical data to measure internal performance of Treasury programs. These numbers are deleted at the end of each project/study. New numbers are randomly created for each study

Specific Information/File Types

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

Audit Log and Security Monitoring Information

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

Medical/Emergency Information Regarding Individuals

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

Biometrics/Distinguishing Features/Characteristics of Individuals

☒ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) Identify which are collected: Gender, Race and National Origin, and Disability	☐ 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):

Applicants who receive and accept job offers for employment with a Federal agency that is serviced by HRC submit the information in Section 4.2 into the USA Staffing using the forms listed in the chart below. These forms are required to complete the hiring/onboarding process. These forms are completed within USA Staffing and some of the information in these forms (not the form itself) is sent to HRC via the New Hire Interconnection. If the New Hire interconnection is not used by one of the Federal Agencies serviced by HRConnect, the data from the paper forms is manually input into HRConnect.

Form	*USA Staffing*	*HRC*
AD-349 USDA Employee Address or TR Employee Address	Yes	Yes
PIV Applicant Information	Yes	No
SF-1199A Direct Deposit / Allotments	Yes	Yes
W4 Federal Tax Withholding	Yes	Yes
All State Tax Withholdings	Yes	Yes
SF-181 Ethnicity and Race Identification	Yes	Yes
SF-256 Self Identification of Disability	Yes	Yes
SF-2809 Federal Employment Health Benefits (FEHB) Election	Yes	Yes
DG 60 FEHB Premium Conversion Waiver	Yes	Yes
SF-2817 Federal Employee Group Life Insurance (FEGLI) Life Insurance Election	Yes	Yes
SF-3109 Federal Employee Retire System (FERS) Election of Coverage	Yes	Yes
SF-1152 Designation of Beneficiary Unpaid Compensation	Yes	No
TSP1 Thrift Savings Plan Election	Yes	Yes
TSP3 Thrift Savings Plan Designation of Beneficiary	Yes	No
24-Hr Personal Accident Insurance Enrollment	Yes	Yes (OCC Only)
OCC Group Life Insurance Enrollment	Yes	Yes (OCC Only)
OCC Short Term Disability Enrollment	Yes	Yes (OCC Only)
SF52 Request for Personnel Action	No	Yes
SF50 Notification of Personnel Action	No	Yes
OF-8 Position Description	No	Yes
USS-1 Uniform Service Status	Yes	No
EDU-01 Education Form	Yes	Yes

Form	*USA Staffing*	*HRC*
TR Veterans Form	Yes	Yes
TR Emergency Contacts	Yes	Yes

From the forms listed above, HRConnect extracts information to allow agencies to perform tasks related to individuals' employment, such as compensation, benefits, and retirement.

Forms can be associated with attachment types in HRConnect within an employee's profile. Based on HRConnect's security measures, only HR specialists and bureau administrators are able to access their forms. Forms can be associated with onboard/security attachments; the data will not be stored in HRC tables.

Form	Description
OF-8 (PD)	Position Description and Signed Position Description Form (OF-8)
RISK LEVEL	OPM's Position Designation Tool Output
ALIEN REGISTRATION	Permanent Alien Registration Card
BIRTH CERTIFICATE	Certificate of Birth
CITIZEN BOARD ABROAD	U.S. Citizen Born Abroad
CONTRACTS	Contracts and Modifications
CSF	Contractor Suitability Form (CSF)
FCRA	Fair Credit Reporting Act (13340)
IPA AGREEMENT	Intergovernmental Personnel Act (IPA) Agreement Form
MOU/MOA	Memorandum of Understanding/Agreement
MTC ACCESS	Application for Access to Main Treasury Complex
NATURALIZATION CERTIFICATE	U.S. Certificate of Naturalization
NDA	Non-Disclosure Agreement
NEW HIRE SELECTION	New Hire Selection Notice
OF-306	Declaration of Federal Employment Form (OF-306)
RESUME	Resume
SF-52	Request for Personnel Action (SF-52)
SUPPLEMENTAL DOCUMENTATION	Supplemental Documentation - Application to MTC or Security Processing
VAR	Visit Access Request
DIPLOMA	Diploma
CERTIFCATE	Certificate of Completion
DIVORCE DEGREE	Divorce Decree
JUSTIFICATION	Justification
MARRIAGE CERT	Marriage Certificate

HRConnect does not maintain actual Federal forms. Federal agencies that use HRC and USA Staffing only maintain data extracted from the federal/agency forms listed in Appendix A which are entered into HRC from the USA Staffing data feed. The table in Appendix A is a complete list of forms and all data elements containing PII associated with each form. Document attachments are allowed in HRConnect.

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*

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

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

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

☒ Federal contractors, interns, detailees etc. *PII is collected from federal contractors, interns, and detailees to complete their background security investigation. Additionally, once they are onboarded, their personal information is retained in HRConnect for traceability and HR purposes. Information for grantees, including but not limited to PII is not collected in HRConnect.*

☒ Federal job applicants. *Applicants who receive and accept job offers for employment (new employees) with a federal agency that is serviced by HRConnect submit information using the forms listed in Section 4.2, which are required to complete the hiring/onboarding process. For those agencies that use the USA Staffing, these forms are completed within USA Staffing and the necessary information (not all information contained in the forms) is sent to HRConnect via an interface. Information from USAS is collected and sent to HRC via Application Programming Interface (API).*

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

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. *PII collected using OPM HSPD-12 form to capture suitability information related to the federal government internship.*

☒ Detailees. *PII collected using OPM HSPD-12 form to capture suitability information related to the federal government detail.*

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

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.).

Other Federal Agencies

☒ Other federal agencies: *A complete list of agencies is listed in Section 3.1*

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).

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.).

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. Please check the statement below that applies to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.

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. 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. (the language provided may require some modification to describe the system or project that is the subject of this PCLIA).

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 (check the appropriate box): ☐ 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 [*login page of the USAS onboarding system*]. *The Privacy Act Statement is provided to new hires on the login page for the USAS onboarding system. The statement from the USAS onboarding login page states, "The Office of Personnel Management is required by the Privacy Act of 1974 (5 U.S.C. 552a) to tell you why OPM is requesting this information."*
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 for collection and use of the full Social Security. Please check the statement below that applies to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.

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

is located anywhere in the system (even if it is redacted, truncated or anonymized when viewed by users, please check number 2 below)].

2. ☒ Full SSNs are maintained in the system or by the project and the following approved Treasury uses of SSNs apply:

   ☐ security background investigations;

   ☒ interfaces with external entities that require the SSN;

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

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

   ☐ statistical and other research purposes;

   ☒ delivery of government benefits, privileges, and services;

   ☐ for law enforcement and intelligence purposes;

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

   ☒ as a unique identifier for identity verification purposes.

Section 4.3(e) Controls implemented to limit access to and or improper disclosure of full Social Security Numbers. ***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. ☐ 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. ☐ N/A No SSNs are maintained in the system or by the project.
2. ☐ Full SSNs are collected, but no individual will be denied any right, benefit, or privilege provided by law if the individual refuses to disclose their SSN for use in the system or project. If the individual chooses not to provide their SSN *[please describe **here** what will happen (something less than denial of a privilege etc.) if the individual chooses not to provide their SSN].*☒ 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: *Applicants who refuse to provide their SSN are denied federal employment. The SSN is required by HRConnect's payroll provider, the United States Department of Agriculture, National Finance Center (NFC). NFC has operated as a payroll system of records since 1973. SSNs are also required for compliance with OPM's adjudication and credentialling standards for issuing Personal Identity Verification (PIV) cards under HSPD-12. If a person refuses to provide their SSN, they will not be able to perform their job duties that require PIV card access*. Denial of this right, benefit or privilege does not violate the law because: [choose one of the two boxes below]:
    a. ☐ SSN disclosure is required by the following Federal statute or Executive Order; **OR**
    b. ☒ The SSN is disclosed to a Federal, state, or local agency that maintains a system of records that was in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

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

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

1. ☒ N/A. The system or project does ***not*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment.
2. ☐ The system or project ***does*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment. *If you checked this box, please check the box below that explains Treasury's authorization for collecting this information:*
    a. ☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance. The individual about whom the

information was collected or maintained expressly authorized its collection by *[explain here how the individual expressly authorizes collection] (for example, individuals may expressly authorize collection by requesting in writing that Treasury share information with a third party, e.g., their Congressman];*

b. ☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity because [generally discuss here the nature and purpose of the information collected and the law enforcement activity];

c. ☐ The following statute expressly authorizes its collection: [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 information collected, maintained, and shared when it is used to make determinations about individuals

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

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

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

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

of the options before checking this box☐ ***None*** of the information maintained in the system or by the project is part of a system of records as defined in section (e)(5) of the Privacy Act, but the information in the system ***is*** used to make adverse determinations about individuals (defined in the Privacy Act as U.S. Citizens and legal permanent residents). Despite the fact that the Privacy Act does not apply, the following protections are in place to ensure fairness to the individual: *explain* ***here*** .

Section 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.
2. ☒ The records maintained by this system or project **are** used to make adverse determinations about individuals ***and*** *[check all that apply]:*

   a. ☐ These records ***were*** exempted from the Privacy Act provision that requires collection directly from the subject individual to the greatest extent practicable. Exemption of these records is proper because *[explain here why the records were exempted; sample responses are provided in Appendix B of this template].*

   b. ☒ These records were ***not*** exempted from the requirement to collect information directly from the individual to the greatest extent practicable ***and***

      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]. Information maintained in the system regarding employee performance may be based on input from both the employee and their manager. Performance information may be used to make an adverse determination about an individual's ability to receive a performance award. For an employee to receive a performance award, they must have received an overall rating of at least fully successful on their performance evaluation. The overall rating is not determined by HRConnect; it is determined (offline) by the manager and reviewing manager during the performance evaluation process. During the performance evaluation process, employees are provided with an opportunity to articulate their performance achievements and may submit an official written statement on their performance evaluation. HRConnect maintains the overall rating and the performance award amount (if any) and electronically transmits both to the payroll provider, NFC. Determinations regarding performance awards, including the amount of individual awards, are made by supervisors and senior staff within each bureau or office.*

      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: (please check all that apply and explain where requested)
   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. ☒ 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. Corrections and amendments made to the record of a Federal employee are done via HR transactions in accordance with the U.S. Office of Personnel Management's Guide to Processing Personnel Actions (GPPA). Individuals are notified via the Standard Form 50 (SF-50), Notification of Personnel Action. For agencies that elect to maintain limited contractor PII in HRConnect, functionality can be enabled for contractors to update/correct their own information directly in HRConnect.*
   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 ☐ before ☒ after it is used to make a final, adverse determination about them. *This is accomplished by adhering to agency policies and procedures for employee relations.*
   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: *HR Specialists and administrators undergo quality assurance process put in place by each agency.*
   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. (please check all that apply and explain where requested)

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: Monday through Friday. The automated data feed updates information when a person onboards and when historical corrections and updates (HCUP packages) are processed. The updates occur to ensure data is accurate and in sync with the payroll provider.

c. ☒ Technical and/or administrative controls put are in place to ensure that when information about an individual is acquired from multiple sources for maintenance in a single file about a particular individual, it all relates to the same individual. This is accomplished by: HRConnect's automated file processing uses the employees Social Security Number (SSN) provided by the payroll provider to identify and match updates to specific employee records since the payroll provider does not maintain unique employee identification numbers.

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

e. ☒ Other: *The data collected is verified for accuracy, relevancy, and completeness by the employees who submit their information to Treasury and other Federal agencies that use HRConnect (and in some cases USA Staffing). The information is also reviewed by participating agencies' HR Specialists and undergoes the quality assurance process put in place by each agency. Treasury employees may also update their information in HRConnect upon request at any time.*

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? Please check the statement below that applies to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.

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. Please check the statement below that applies to your system or project and provide the additional information requested for each box you checked. Please read all possible responses before selecting an answer.

1. ☐ The PII maintained in the system or by the project ***is not*** part of a Privacy Act system of records.
2. ☒ The information maintained in the system or by the project ***is*** part of a Privacy Act system of records, but ***is not*** used as part of a matching program.
3. ☐ The information maintained in the system or by the project ***is*** part of a Privacy Act system of records and ***is*** used as part of a matching program. [*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? Please check the statement below that applies to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.

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:
   - *Department of Veterans Affairs Office of Inspector General Department of Agriculture*
   - *USDA Office Chief Info Officer – CTS (Client Technology Services)*
   - *U. S. Agency for International Development (USAID)*
   - *Architectural and Transportation Barriers Compliance Board (US Access Board)*
   - *Department of Commerce:*
     - *Office of the Secretary*
     - *Economic Development Administration*
     - *Bureau of Economic Analysis*
     - *National Oceanic and Atmospheric Administration*
     - *International Trade Administration*

        - *U. S. Patent and Trademark Office*
        - *National Institute of Standards and Technology*
        - *Minority Business Development Agency*
        - *National Telecommunications and Information Administration*
        - *National Technical Information Service*
        - *Bureau of the Census*
        - *Office of the Inspector General*
        - *Office of Inspector General*
        - *Bureau of Industry and Security*
- *Department of Justice Bureau of Alcohol, Tobacco, Firearms, and Explosives*
- *Department of Labor*
- *Denali Commission*
- *Federal Reserve Bureau of Consumer Financial Protection (BCFP)*
- *Gulf Coast Ecosystem Restoration Council (GCERC)*
- *Office of Government Ethics (OGE)*
- *Federal Housing Finance Agency OIG (FHFA OIG)*
- *Department of Homeland Security U.S. Secret Service (USSS)*
- *Department of Housing and Urban Development (HUD)*
- *Department of Housing and Urban Development HUD Office Inspector General*
- *Government Accountability Office (GAO)*
- *United States Congress Commission on Security and Cooperation in Europe (CSCE)*
- *Armed Services Retirement Home (AFRH)*
- *Federal Mine Safety and Health Fed Mine Safety Health Rev Com*
- *Commission on People's Republic of China (CECPRC)*
- *Veterans Affairs Office of Inspector General (VA OIG)*

Treasury is a cross-services provider to other Treasury bureaus and Federal agencies pursuant to the U.S. Office of Personnel Management Human Resources Line of Business (HRLOB). An Interconnection Security Agreement (ISA) is countersigned by the Servicing Agency (Treasury) and the Requesting Agency (customer). The ISA documents the limits, conditions, and proper usage of the application and the data within by both the Servicing Agency and the Requesting Agency. As the Servicing Agency, Treasury provides data to the third- party application administrators listed below. There are agreements signed between Treasury and these third-party application administrators.

Contracts are also executed between Treasury offices and vendors who perform studies to allow the development of aggregate/statistical data to measure internal performance of Treasury programs. These contractors receive raw data from the system for the limited purpose of conducting the study and developing aggregate statistical data. These contracts limit the vendor's use and disclosure of the data provided, including PII. The vendors are required to safeguard all data and other information, including PII received from the system. Vendors are also prohibited from using or disseminating such data and information for any purpose other than providing the services referenced in the contracts. The contracts also contain confidentiality provisions which prohibit vendor disclosure of any information obtained or prepared in the course of performing services under the contract. At the termination of the contract, vendors are required to return all data provided upon request by Treasury. All government furnished information provided in conjunction with required performance under these contracts must be immediately

returned at the written request of the Government after the purpose of the contract is completed (or before if terminated).

Internal and External HRC customers access their own information directly in HRConnect. When an HRC customer accesses their own information it is not, technically internal sharing; it is merely a use of their own information. HRC customers do, however, sometimes make their own arrangements with vendors outside their organization to share HRC data for the purpose of conducting organizational, workforce, and similar assessments and studies. In general, data is used to develop aggregate/statistical data to measure internal performance of programs and operations. OHR provides customer service with respect to these disclosures upon request, and in accordance with the specific needs of each disclosure. For example, OHR assigns and maintains randomly assigned unique identifiers to each personnel file that is shared internally or externally to allow the development of aggregate/statistical data. These numbers are deleted at the end of each project/study. New unique identifying numbers for personnel files are randomly created for each study.

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) 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 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 *the information contained in this system is being gathered from individuals who have been offered employment with the Federal government, in their capacity as Federal employees, and from current Federal employees. Following an offer of employment, they are no longer considered members of the public, and as such, the Paperwork Reduction Act does not apply*.

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) 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 records used in the system or by the project are covered by a NARA's General Records Schedule (GRS). *Treasury retains Human Resources records in this system in compliance with General Records Schedule (GRS) 2.0, approved by the National Archives and Records Administration (NARA). After GRS 2.7 is approved, GRS 2.7 will govern the disposal of Treasury vaccination records. HRConnect will retain and dispose OGE 450 financial records as outlined in NARA GRS 2.8.*
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) 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 is a federal information system subject to FISMA requirements.
2. ☒The system last completed an SA&A and received an ATO on: 1/31/2020
3. ☐This is a new system has not yet been authorized to operate. The expected to date for receiving ATO is *[please state here the expected date on which you expect authorization will be granted].*
4. ☒ The system or project maintains access controls to ensure that access to PII maintained is limited to individuals who have a need to know the information in order to perform their official Treasury duties. *Access to the data by a user is determined based upon the roles assigned to the user's profile. Roles are assigned based on position. Specifically, users will only have access to the data that is inherently theirs, such as their own personally identifiable information (PII). In the case of managers, they will have access to their own PII as well as limited information of those employees assigned to them. Additional roles may be assigned using strict 'need-to-know' criteria. The criteria, procedures, controls, and responsibilities regarding access are documented.*
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. *The data in the system is shared with data owners (both internal and external to Treasury). These individuals must access the URL address via a secure and recognized connection to the Treasury network gateway and authenticate to the application using multi-factor authentication. Authorized third parties receive extracts of data in the system based on a 'need-to-know' basis and in accordance with a written agreement between themselves and the U.S. Department of Treasury, Office of the Chief Information Office, Enterprise Business Solutions, and HRConnect Program Office. The agencies must then adhere to the prescribed configuration management principles and procedures in conjunction with the HRConnect Program Office information systems protocols to set up a periodic file feed with the extracted information. In support of the HSPD-12 Initiative, HRConnect implemented an application programming interface (API) platform to provide data exchange services.*
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. *HRConnect is based on a COTS product (Oracle PeopleSoft). The COTS product platform for HRConnect has been evaluated by Oracle using the Voluntary Product Accessibility Template (VPAT). The Voluntary Product Accessibility Template (VPAT) was developed by ITI and GSA to assist Federal contracting officials and other buyers in making preliminary assessments regarding the availability of commercial Information and Communication Technology (ICT) products and services with features that support accessibility*.
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

Srikaran Chilukuri
Director, Human Resources Information Technology Development and Application Services
Enterprise Applications
HRConnect System Owner
U.S. Department of the Treasury

Nicolaos Totten
Deputy Chief Information Officer for Applications and Digital Services
Enterprise Applications
HRConnect Authorizing Official
U.S. Department of the Treasury

Approval Signature

_____
Timothy H. Skinner, JD
Bureau Privacy and Civil Liberties Officer
Office of Privacy, Transparency, & Records

Appendix A: Forms and Data Elements

Form ID	What is being captured?	Data Elements
Ethnicity and Race Identification (SF-181)	*All data elements of SF-181 pertaining to the applicant are collected*	Applicant Name
		Social Security Number
		Date of Birth
		Ethnicity / Race
Self-Identification of Disability (SF-256)	*All data elements of SF-256 pertaining to the applicant are collected*	Applicant Last Name, First Name, and Middle Initial
		Date of Birth
		Social Security Number
Direct Deposit Sign-Up (SF-1199A)	*Data elements in SF-1199A pertaining to the Applicant and Joint Payee and Joint Account holder information is collected*	Applicant Name of Payee Last, First, Middle Name
		Name of person entitled to payment
		Depositor account number
		Applicant address
		Applicant claim or Payroll ID number
		Joint Account holders certification required signature
		Applicant Telephone number
		Payee / Joint Payee Certification require signature
		Type of Depositor Account Checking or Savings
FERS Election of Coverage (SF-3109)	*Data elements in SF-3109 pertaining to the Applicant and Former Spouse Information is collected*	Applicant Name (Last, First, Middle)
		Applicant Social Security Number
		Applicant Date of Birth
		Applicant Marital Status
		Applicant Former Spouse's Full Name (if OPM Form 1556) is included as an attachment)
Designation of Beneficiary Unpaid Compensation of Deceased Civilian Employee (SF-1152)	*Data elements in SF-1152 pertaining to the Applicant and Beneficiary for the Applicant are collected*	Applicant Name (Last, First, Middle Name)
		Applicant Address
		Address of Each Applicant Beneficiary
		Applicant Date of Birth
		Applicant Beneficiary (First Name, Middle Initial, and Last Name) of Each Beneficiary
		Beneficiary Relationship to Applicant
		Applicant Social Security Number
Thrift Saving Plan Designation of Beneficiary (TSP-3)	*Data elements in TSP-3 pertained to the Applicant and Beneficiary are collected*	Applicant Name (Last, First, Middle)
		Applicant Foreign Address
		Applicant Foreign Address
		Applicant Beneficiary Social Security Number or Tax ID
		Applicant TSP Account Number
		Applicant Benefits Information (including optional benefits selected)

Form ID	What is being captured?	Data Elements
		Applicant Beneficiary Date of Birth
		Applicant Date of Birth
		Applicant Relationship to Beneficiary information: Name of Spouse, Trust, Estate, Legal Entity / Corporation
		Applicant Beneficiary Foreign Address
		Applicant Day Time Phone Number
		Applicant Beneficiary Name of Individual Last, First, Middle / Legal Entity or Corporation
		Applicant Beneficiary Home Address
		Applicant Home Address
Employee Election Form (TSP-1)	*All data elements of TSP-1 pertaining to the applicant are collected*	Applicant Name (Last, First, Middle)
		Address
		Social Security Number
		Home Phone Number
Premium Conversion Waiver / Election (DG-60)	*All data elements of DG-60 pertaining to the applicant are collected*	Applicant Name (Last, First, Middle Initial)
		Applicant Social Security Number
		Applicant Phone Number
Life / Health Insurance / Benefits (SF-2809)	*Data elements in SF-2809 pertaining to the Applicant and Eligible Family Member(s) are collected*	Applicant/Enrollee Name (Last, First, Middle Initial)
		Applicant Social Security Number
		Applicant Date of Birth
		Applicant Gender
		Applicant Marital Status
		Applicant Home Address
		Applicant Name of other Insurance and Policy Number
		Applicant Policy Number
		Applicant Email Address
		Applicant Phone Number
		Eligible Family Member(s) Name (Last, First, Middle Initial)
		Eligible Family Member(s) Social Security number
		Eligible Family Member(s) Date of Birth
		Eligible Family Member(s) Gender
		Eligible Family Member(s) Address
		Eligible Family Member(s) Name of Other Insurance
		Eligible Family Member(s) Name of Other Insurance and Policy Number
		Eligible Family Member(s) Medicare Claim Number
		Eligible Family Member(s) Email Address
Life Insurance Election (FEGLI) (SF-2817)	*All data elements of SF-2817 pertaining to the applicant are collected*	Applicant Name (Last, First, Middle)
		Applicant Date of Birth
		Applicant Social Security Number

Form ID	What is being captured?	Data Elements
		Office of Worker's Compensation Programs (OWCP)
		Applicant Telephone Number
Withholding Allowances / Exemption Certificate (W-4)	*All data elements of W-4 pertaining to the applicant are collected*	Employee Name (First, Middle Initial, Last Name)
		Employee Address
		Employee Home Address
		Employee Marital Status
AD-349	*Data elements pertaining to applicant address are collected*	Name (Last, First, Middle)
		Employee Mailing Address
		Employee Address
		Social Security Number
		Signature of Employee
		Employee Home Address
Personal Identity Verification for Federal Employees and Contractors (Form 13760)	*Not all data elements in Form 13760 are collected*	Employee Status (Employee or Contractor)
		Contract Number
		Contractor's Company Name
		Name (Last, First, Middle Initial)
		Social Security Number
		Date of Birth
		Home Mailing Address
		Signature
		Sponsor Name
		Sponsor Title
		Sponsor Phone Number
		Sponsor Signature
		ID Number
		Registrar Name
		Registrar Title
		Registrar Phone Number
		Registrar Signature
		Issuer Name
		Issuer Title
		Issuer Phone Number
		Issuer Signature
Certificate of Non-Residence in the District of Columbia (Form D-4A)	*Not all data elements in Form D-4A are collected*	Name (First Name, Middle Initial, Last Name)
		Temporary DC Address
		Social Security Number
		Permanent Address
		Signature
	Not all data elements in Form SF-50 are collected	Name (Last, First, Middle)
		Social Security Number

Form ID	What is being captured?	Data Elements
Notification of Personnel Action (SF-50)		Date of Birth
		Position Title and Number
		Pay Plan
		Occ. Code
		Grade or Level
		Step or Rate
		Total Salary
		Pay Basis
		Name and Location of Position's Organization
		Veterans Preference
		Tenure
		FEGLI
		Service Computation Date
		Work Schedule
		Position Occupied
		FLSA Category
		Appropriation Code
		Bargaining Unit Status
		Duty Station
		Employing Department or Agency
		Signature and Title of Approving Official
Confidential Financial Disclosure Report (OGE Form 450)	*Not all data elements in OGE Form 450 are collected.*	Name (Last, First, Middle Initial)
		Position / Title
		Agency
		Branch / Unit and Address
		Work Number
		Email Address
		Special Government Employee (SGE)
		SGE Mailing Address
		Reporting Status
		Certifying Individual's Signature
		Reviewer's Signature
		Agency's Final Reviewing Official's Signature
		Assets and Income Amounts
		Transactions Exceeding $1,000
		Gifts, Reimbursements, and Travel Expenses
		Debts over $10,000
		Other Employment Compensation
		Employment Held Outside of the U.S. Government