



Privacy and Civil Liberties Impact Assessment  
for the

## HR Connect SYSTEM

October 2016

### **Reviewing Official**

Ryan Law

Acting Deputy Assistant Secretary for Privacy, Transparency, and  
Records

Department of the Treasury

### **Bureau Certifying Official**

Timothy H. Skinner, J.D., CIPP/G/US/EU  
Bureau Privacy and Civil Liberties Officer  
Office of Privacy, Transparency, & Records  
Department of the Treasury

## Section 1: Introduction

It is the policy of the Department of the Treasury (“Treasury” or “Department”) and its Bureaus to conduct a Privacy and Civil Liberties Impact Assessment (“PCLIA”) when personally identifiable information (“PII”) is maintained in a system or by a project. PCLIA’s are required for all systems and projects that collect, maintain, or disseminate PII, regardless of the manner in which the information is retrieved.

This assessment is being completed 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. Agencies, instrumentalities, or employees of the federal government are not included.

This PCLIA provides the following information regarding the system or project:

- (1) an overview of its purpose and functions;
- (2) a description of the information collected;
- (3) a description of the how information is maintained, used, and shared;
- (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and
- (5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

This PCLIA supersedes the Privacy Impact Assessment for this system dated June 13, 2011.

## Section 2: Definitions

**Agency** – means any entity that falls within the definition of the term “executive agency” as defined in 31 U.S.C. § 102.

**Certifying Official** – The Bureau Privacy and Civil Liberties Officer(s) who certify that all requirements in TD and TD P 25-07 have been completed so a PCLIA can be reviewed and approved by the Treasury Deputy Assistant Secretary for Privacy, Transparency, and Records.

**Collect (including “collection”)** – means the retrieval, receipt, gathering, or acquisition of any PII and its storage or presence in a Treasury system. This term should be given its broadest possible meaning.

**Contractors and service providers** – are private companies that provide goods or services under a contract with the Department of the Treasury or one of its bureaus. This includes, but is not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

**Data mining** – means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where – (a) a department or agency of the federal government, or a non-federal entity acting on behalf of the federal government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely – (i) the detection of fraud, waste, or abuse in a government agency or program; or (ii) the security of a government computer system.

**Disclosure** – When it is clear from its usage that the term “disclosure” refers to records provided to the public in response to a request under the Freedom of Information Act (5 U.S.C. § 552, “FOIA”) or the Privacy Act (5 U.S.C. § 552a), its application should be limited in that manner. Otherwise, the term should be interpreted as synonymous with the terms “sharing” and “dissemination” as defined in this manual.

**Dissemination** – as used in this manual, is synonymous with the terms “sharing” and “disclosure” (unless it is clear from the context that the use of the term “disclosure” refers to a FOIA/Privacy Act disclosure).

**E-Government** – means the use of digital technologies to transform government operations to improve effectiveness, efficiency, and service delivery.

**Federal information system** – means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information owned or under the control of a federal agency, whether automated or manual.

**Final Rule** – After the NPRM comment period closes, the agency reviews and analyzes the comments received (if any). The agency has the option to proceed with the rulemaking as proposed, issue a new or modified proposal, or withdraw the proposal before reaching its final decision. The agency can also revise the supporting analyses contained in the NPRM (e.g., to address a concern raised by a member of the public in response to the NPRM).

**Government information** – means information created, collected, used, maintained, processed, disseminated, or disposed of by or for the federal government.

**Individual** – means a citizen of the United States or an alien lawfully admitted for permanent residence. If a question does not specifically inquire about or an issue does not clearly involve a [Privacy Act system of records](#), the term should be given its common, everyday meaning. In certain contexts, the term individual may also include citizens of other countries who are covered by the terms of an international or other agreement that involves information stored in the system or used by the project.

**Information** – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. This term includes, but is not limited to, information contained in a [Privacy Act system of records](#).

**Information technology (IT)** – means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support

services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).

**Major Information system** – embraces “large” and “sensitive” information systems and means “a system or project that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.” OMB Circular A-130, § 6.u. This definition includes all systems that contain [PII](#) and are rated as “MODERATE or HIGH impact” under Federal Information Processing Standard 199.

**National Security systems** – a telecommunications or information system operated by the federal government, the function, operation or use of which involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management. Clinger-Cohen Act of 1996, 40 U.S.C. § 11103.

**Notice of Proposed Rule Making (NPRM)** – the Privacy Act (Section (J) and (k)) allow agencies to use the rulemaking process to exempt particular systems of records from some of the requirements in the Act. This process is often referred to as “notice-and-comment rulemaking.” The agency publishes an NPRM to notify the public that the agency is proposing a rule and provides an opportunity for the public to comment on the proposal before the agency can issue a final rule.

**Personally Identifiable Information (PII)** –any information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

**Privacy and Civil Liberties Impact Assessment (PCLIA)** – a PCLIA is:

- (1) a *process* conducted to: (a) identify privacy and civil liberties risks in systems, programs, and other activities that maintain [PII](#); (b) ensure that information systems, programs, and other activities comply with legal, regulatory, and policy requirements; (c) analyze the privacy and civil liberties risks identified; (d) identify remedies, protections, and alternative or additional privacy controls necessary to mitigate those risks; and (e) provide notice to the public of privacy and civil liberties protection practices.
- (2) a *document* that catalogues the outcome of that privacy and civil liberties risk assessment process.

**Protected Information** – as the term is used in this PCLIA, has the same definition given to that term in TD 25-10, Section 4.

**Privacy Act Record** – any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual’s education, financial transactions, medical history, and criminal or employment history and that contains the individual’s name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. 5 U.S.C. § 552a(a)(4).

**Reviewing Official** – The Deputy Assistant Secretary for Privacy, Transparency, and Records who reviews and approves all PCLIA as part of her/his duties as a direct report to the Treasury Senior Agency Official for Privacy.

**Routine Use** – with respect to the disclosure of a record outside of Treasury (i.e., external sharing), the sharing of such record for a purpose which is compatible with the purpose for which it was collected 5 U.S.C. § 552a(a)(7).

**Sharing** – any Treasury initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of Treasury information, regardless of whether it is covered by the Privacy Act. It does not include responses to requests for agency records under FOIA or the Privacy Act. It is synonymous with the term “dissemination” as used in this assessment. It is also synonymous with the

term “disclosure” as used in this assessment unless it is clear from the context in which the term is used that it refers to disclosure to the public in response to a request for agency records under FOIA or the Privacy Act.

**System** – as the term used in this manual, includes both federal information systems and information technology.

**System of Records** – a group of any records under the control of Treasury from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. 5 U.S.C. § 552a (a)(5).

**System of Records Notice** – Each agency that maintains a system of records shall publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records, which notice shall include: (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at her/his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at her/his request how she/he can gain access to any record pertaining to him contained in the system of records, and how she/he can contest its content; and (I) the categories of sources of records in the system. 5 U.S.C. § 552a (e)(4).

**System Owner** – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

## [Section 3: System Overview](#)

### [Section 3.1: System/Project Description and Purpose](#)

The purpose of the HR Connect system is to support the human resources functions for the Department of the Treasury and other federal agencies that use HR Connect as part of a cross-services initiative to reduce federal government expenditures. The federal agencies (or components of those agencies) that use HR Connect are:

- Consumer Financial Protection Bureau (CFPB)
- Department of Commerce
- Department of Housing and Urban Development (HUD)
- Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives
- Department of Labor
- Department of Homeland Security, US Secret Service (DHS USSS)
- Department of the Treasury
- The Government Accountability Office (GAO)
- United States Agency for International Development (USAID)

#### **Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project**

- |   |  |  |
|---|--|--|
| <input type="checkbox"/> 0 – 999                      | <input type="checkbox"/> 1000 – 9,999      | <input type="checkbox"/> 10,000 – 99,999 |
| <input checked="" type="checkbox"/> 100,000 – 499,999 | <input type="checkbox"/> 500,000 – 999,999 | <input type="checkbox"/> 1,000,000+      |

## [Section 3.2: Authority to Collect](#)

The authorities for operating this system or performing this project are:

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.

31 U.S.C. 321—General authorities of the Secretary establish the mission of the Department of the Treasury.

Homeland Security Presidential Directive 12 (HSPD-12) – requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors.

Treasury Directive 80-05, Records and Information Management Program – establishes the policy of the Department of the Treasury to manage records effectively and efficiently throughout their life cycle in order to facilitate accomplishment of the agency's programmatic and administrative missions, to preserve official agency records in accordance with applicable statutory and regulatory requirements, and to ensure access to information by Treasury officials, and the public as appropriate.

## [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 fulfilled 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\(a\)](#)** Please check all of the following that are true:

- None of the [PII](#) maintained in the system or by the project is part of a [Privacy Act system of records](#);
- All of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and none of it is exempt from the [Privacy Act](#) relevant and necessary requirement;
- All of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and all of it is exempt from the [Privacy Act](#) relevant and necessary requirement;
- Some, but not all, of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and the records to which the [Privacy Act](#) applies are exempt from the relevant and necessary requirement; and  
 Some, but not all, of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and none of the records to which the [Privacy Act](#) applies are exempt from the relevant and necessary requirement.

**[Section 4.1\(b\)](#)**  Yes  No  N/A With respect to [PII](#) maintained in the system or by the project that is subject to the [Privacy Act's](#) relevant and necessary requirement, was an assessment conducted prior to collection (e.g.,

during [Paperwork Reduction Act](#) analysis) to determine which [PII](#) types (see [Section 4.2](#) below) were relevant and necessary to meet the system's or project's mission requirements?

[Section 4.1\(c\)](#)  Yes  No  N/A With respect to [PII](#) currently maintained in the system or by the project that is subject to the [Privacy Act's](#) relevant and necessary requirement, is the [PII](#) limited to only that which is relevant and necessary to meet the system's or project's mission requirements?

[Section 4.1\(d\)](#)  Yes  No With respect to [PII](#) maintained in the system or by the project that is subject to the [Privacy Act's](#) relevant and necessary requirements, is there a process to continuously reevaluate and ensure that the [PII](#) remains relevant and necessary?

*All data elements pertaining to human resources information have been detailed within HR Connect and PIV Data Synchronization (PDS) Data Model [data dictionary](#) and documented pursuant to the requirements imposed by Office of Management and Budget (OMB) Circular A-130. Additionally, all of the data elements are part of the functional requirements documentation and the configuration management procedures being adhered to by Treasury. Functional requirements documentation consists of data elements, valid values, business rules, workflow, and interfaces that define a given set of functionality within the system. Configuration management procedures are a set of processes, templates, guidelines, and frameworks used to create a snapshot of what the application configuration and code looks like at a given point in time and to plan what the application configuration and code will look like at a defined point in the future (i.e., release).*

*HR Connect also collects information using the forms listed in the table below which are subject to the Paperwork Reduction Act. Forms that are subject to the PRA must be approved by the Director of the Office of Management and Budget (OMB) before they are used to collect information from the public. The OMB Director is required by law to determine whether a proposed collection of information by the agency is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility to the agency. If the OMB Director determines that the collection of information (or a portion of the information proposed for collection) by an agency is unnecessary for any reason, the agency may not engage in the collection of that information. All information that is collected in HR Connect using forms subject to the PRA have been approved by the OMB Director and, therefore, been assessed and determined to be relevant and necessary.*

*The HR Connect system permits the individual to update their data throughout their employment to keep it current.*

## [Section 4.2: PII and/or information types or groupings](#)

To perform their various missions, federal agencies must necessarily collect various types of information. The checked boxes below represent the types of information maintained in the system or by the project. Information identified below is used by the system or project to fulfill the purpose stated in [Section 3.2](#) – Authority to Collect.

<b>Biographical/General Information</b>		
<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Gender	<input type="checkbox"/> Group/Organization Membership
<input checked="" type="checkbox"/> Date of Birth	<input checked="" type="checkbox"/> Race	<input checked="" type="checkbox"/> Military Service Information
<input checked="" type="checkbox"/> Home Physical/Postal Mailing Address	<input checked="" type="checkbox"/> Ethnicity	<input checked="" type="checkbox"/> Personal Home Phone or Fax Number
<input checked="" type="checkbox"/> Zip Code	<input checked="" type="checkbox"/> Personal Cell Number	<input type="checkbox"/> Alias (including nickname)
<input type="checkbox"/> Business Physical/Postal Mailing Address	<input checked="" type="checkbox"/> Business Cell Number	<input checked="" type="checkbox"/> Business Phone or Fax Number
<input checked="" type="checkbox"/> Personal e-mail address	<input type="checkbox"/> Nationality	<input type="checkbox"/> Mother's Maiden Name
<input type="checkbox"/> Business e-mail address	<input checked="" type="checkbox"/> Country of Birth	<input checked="" type="checkbox"/> Spouse Information
<input type="checkbox"/> Personal Financial Information (including loan information)	<input checked="" type="checkbox"/> City or County of Birth	<input type="checkbox"/> Children Information
<input type="checkbox"/> Business Financial	<input type="checkbox"/> Immigration Status	<input type="checkbox"/> Information about other

Information (including loan information)

Marital Status

Citizenship

Religion/Religious Preference

Device settings or preferences (e.g., security level, sharing options, ringtones).

Sexual Orientation

User names, avatars etc.

Cell tower records (e.g., logs, user location, time etc.)

Network communications data

Contact lists and directories (known to contain personal information)

Contact lists and directories (not known to contain personal information, but uncertain)

Education Information

Resume or curriculum vitae

Other (please describe):

Other (please describe):

relatives.

Professional/personal references or other information about an individual's friends, associates or acquaintances.

Global Positioning System (GPS)/Location Data

Secure Digital (SD) Card or Other Data stored on a card or other technology

Cubical or office number

Contact lists and directories (known to contain only business information)

Other (please describe):

Other (please describe):

### Identifying Numbers

Full Social Security number

Health Plan Beneficiary Number

Truncated/Partial Social Security number (e.g., last 4 digits)

Alien Registration Number

Personal Taxpayer Identification Number

Business Taxpayer Identification Number (If known:  sole proprietor;  non-sole proprietor)

Personal Credit Card Number

Business Credit Card Number (If known:  sole proprietor;  non-sole proprietor)

Personal Vehicle Identification Number

Business Vehicle Identification Number (If known:  sole proprietor;  non-sole proprietor)

Personal License Plate Number

Business License Plate Number (If known:  sole proprietor;  non-sole proprietor)

File/Case ID Number (individual)

File/Case ID Number (business) (If known:  sole proprietor;  non-sole proprietor)

Personal Professional License Number

Business Professional License Number (If known:  sole proprietor;  non-sole proprietor)

Employee Identification Number

Patient ID Number

Business Bank Account Number

Personal Bank Account Number

Commercially obtained internet navigation/purchasing habits of individuals

Government obtained internet navigation/purchasing habits of individuals

Business License Plate Number (non-sole-proprietor)

Driver's License Number

Personal device identifiers or serial numbers

Other Identifying Numbers (please describe): \_\_\_\_\_

Passport Number and Passport information (including full name, passport number, DOB, POB, sex, nationality, issuing country photograph and signature) (use "Other" if some but not all elements are collected)

Other Identifying Numbers (please describe): \_\_\_\_\_

### Medical/Emergency Information Regarding Individuals



- |   |  |   |
|---|--|---|
| <input type="checkbox"/> Medical/Health Information     | <input type="checkbox"/> Worker's Compensation Act Information | <input type="checkbox"/> Patient ID Number  |
| <input type="checkbox"/> Mental Health Information      | <input type="checkbox"/> Disability Information                | <input checked="" type="checkbox"/> Emergency Contact Information (e.g., a third party to contact in case of emergency) |
| <input type="checkbox"/> Other (please describe): _____ |  |   |

### Biometrics/Distinguishing Features/Characteristics of Individuals

- |  |   |   |
|--|---|---|
| <input type="checkbox"/> Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) | <input type="checkbox"/> Signatures                     | <input type="checkbox"/> Vascular scans                 |
| <input type="checkbox"/> Fingerprints  | <input type="checkbox"/> Photos                         | <input type="checkbox"/> Retina/Iris Scans              |
| <input type="checkbox"/> Palm prints   | <input type="checkbox"/> Video                          | <input type="checkbox"/> Dental Profile                 |
| <input type="checkbox"/> Voice audio recording   | <input type="checkbox"/> Scars, marks, tattoos          | <input type="checkbox"/> DNA Sample or Profile          |
| <input type="checkbox"/> Other (please describe): _____  | <input type="checkbox"/> Other (please describe): _____ | <input type="checkbox"/> Other (please describe): _____ |

### Specific Information/File Types

- |  |  |  |
|--|--|--|
| <input type="checkbox"/> Taxpayer Information/Tax Return Information                           | <input type="checkbox"/> Law Enforcement Information   | <input type="checkbox"/> Security Clearance/Background Check Information |
| <input type="checkbox"/> Civil/Criminal History Information/Police Records (government source) | <input type="checkbox"/> Credit History Information (government source)                          | <input type="checkbox"/> Bank Secrecy Act Information                    |
| <input type="checkbox"/> Civil/Criminal History Information/Police Records (commercial source) | <input type="checkbox"/> Credit History Information (commercial source)                          | <input type="checkbox"/> National Security/Classified Information        |
| <input type="checkbox"/> Protected Information (as defined in Treasury Directive 25-10)        | <input type="checkbox"/> Case files  | <input checked="" type="checkbox"/> Personnel Files                      |
| <input type="checkbox"/> Information provided under a confidentiality agreement                | <input type="checkbox"/> Information subject to the terms of an international or other agreement | <input type="checkbox"/> Other (please describe): _____                  |

### Audit Log and Security Monitoring Information

- |   |   |  |
|---|---|--|
| <input checked="" type="checkbox"/> User ID assigned to or generated by a user of Treasury IT   | <input type="checkbox"/> Date and time an individual accesses a facility, system, or other IT | <input type="checkbox"/> Files accessed by a user of Treasury IT (e.g., web navigation habits) |
| <input type="checkbox"/> Passwords generated by or assigned to a user of Treasury IT  | <input type="checkbox"/> Internet or other queries run by a user of Treasury IT               | <input type="checkbox"/> Contents of files accessed by a user of Treasury IT                   |
| <input type="checkbox"/> Biometric information used to access Treasury facilities or IT   | <input type="checkbox"/> Video of individuals derived from security cameras                   | <input type="checkbox"/> Public Key Information (PKI).   |
| <input type="checkbox"/> Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT or devices | <input type="checkbox"/> Still photos of individuals derived from security cameras.           | <input type="checkbox"/> Internet Protocol (IP) Address  |
| <input type="checkbox"/> Other (please describe): _____   | <input type="checkbox"/> Other (please describe): _____                                       | <input type="checkbox"/> Other (please describe): _____  |

Other

Other (please describe: \_\_\_\_\_)  
 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 HR Connect submit information using the forms listed below that are required to complete the hiring/onboarding process:

- AD- 349 Employee Address
- All fifty plus state tax forms
- D4A – DC Tax Waiver
- DG 60 FEHB Premium Conversion Waiver
- DS5002 - Foreign Service Designation of Beneficiary Form
- I-9 Employment Eligibility Verification Data form
- OF-306 Declaration for Federal Employment
- OGE-278e Executive Branch Personnel Public Financial Disclosure Report
- OGE 450 Confidential Financial Disclosure
- PIV Applicant Information
- SF-50 Notification of Personnel Action
- SF-61 Appointment Affidavit/Oath of Office
- SF-144 Statement of Prior Federal Service
- SF-181 Ethnicity and Race Identification
- SF-256 Self Identification of Disability
- SF-1152 Designation of Beneficiary Unpaid Compensation
- SF-1199A Direct Deposit
- SF-2808 Designation of Beneficiary – Civil Service Retirement System (CSRS)
- SF-2809, Health Benefits Election Form
- SF-2817 FEGLI Life Insurance Election
- SF-2823 FEGLI Designation of Beneficiary
- SF-3109 Federal Employees Retirement System (FERS) Election of Coverage
- SF-3102 Designation of Beneficiary – Federal Employees Retirement System (FERS)
- TSP1 Thrift Savings Plan Election
- TSP1-C Thrift Savings Plan Catch-Up
- TSP3 Designation of Beneficiary – Thrift Savings Plan (TSP)
- TSP-19 Transfer
- W4 Federal Withholding

These forms require individuals to submit personally identifiable information (PII). The data submitted is entered into HR Connect for purposes of performing activities related to individuals' employment, such as compensation, benefits, and retirement. This includes the following types of information:

- Personal Identifiable Data
- Emergency Contact Data
- Citizenship, Race & Ethnicity Data
- Disability Data
- Banking & Financial Data
- Federal & State Tax Data
- Selective Service and Military Service Data
- Criminal and Debt History Data related to suitability for employment
- Education Data
- Beneficiary & Dependent Data
- Health Benefit Data

The table below is a complete list of HR Connect forms and all PII data elements associated with each form.

<b>Form ID</b>	<b>Form Name</b>	
<b>General Onboarding Forms</b>		
<i>Declaration for Federal Employment</i>		
<a href="#"><u>OF-306</u></a>	<b>Declaration for Federal Employment</b>	<b>All Data Elements in OF-306 pertain to the Applicant</b>
Applicant Full name (if only have initials in name provide and indicate “initials only”; if no middle name indicate “No Middle Name”)	Phone Number	Selective Service Registration
Social Security Number	Date of birth	Branch of Service
Place of Birth	Other Names used	Dates of Military Service
Citizenship	Military Service	Type of Discharge
Other Names used		
<i>Appointment Affidavit</i>		
<a href="#"><u>SF-61</u></a>	<b>Appointment Affidavit</b>	<b>All Data Elements in SF-61 pertain to the Applicant</b>
Applicant Name	Notary Public Commission Seal information	
<i>Statement of Prior Federal Service</i>		
<a href="#"><u>SF-144</u></a>	<b>Statement of Prior Federal Service</b>	<b>All Data Elements in SF-144 pertain to the Applicant</b>
Applicant Name Last, First, Middle	Date of Birth	Year, month and day of service
Social Security Number	Branch of Uniformed service	Type of Discharge
<i>Ethnicity and Race Identification</i>		
<a href="#"><u>SF-181</u></a>	<b>Ethnicity and Race Identification</b>	<b>All Data Elements in SF-181 pertain to the Applicant</b>
Applicant Name	Social Security Number	Date of Birth
Ethnicity/Race		
<i>Self-Identification of Disability</i>		
<a href="#"><u>SF-256</u></a>	<b>Self-Identification of Disability</b>	<b>All Data Elements in SF-256 pertain to the Applicant</b>
Applicant Last Name, First Name, and Middle initial	Date of Birth	Social Security Number
<i>Direct Deposit Sign-up</i>		
<a href="#"><u>SF-1199A</u></a>	<b>Direct Deposit Sign-Up</b>	<b>Data Elements in SF-1199A pertain to the Applicant and Joint Payee and Joint Account holder information</b>
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
<i>FERS Election of Coverage</i>		
<a href="#"><u>SF-3109</u></a>	<b>FERS Election of Coverage</b>	<b>Data Elements in SF-3109 pertain to the Applicant and Former Spouse Information</b>
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	
<b><i>Designation of Beneficiary (CSRS)</i></b>		
<b><u>SF-2808</u></b>	<b>Designation of Beneficiary (CSRS)</b>	<b>Data Elements in SF-2808 pertain to Applicant and Designation for beneficiary or beneficiaries</b>
Applicant Name Last, First, Middle	Applicant Retirement Claim Number	Address of each beneficiary
Applicant Date of Birth	Applicant Address	Relationship to applicant
Applicant Social Security Number	Applicants Designation for beneficiary or beneficiaries First name, middle initial, and last name of each beneficiary	
<b><i>Designation of Beneficiary (FEGLI)</i></b>		
<b><u>SF-2823</u></b>	<b>Designation of Beneficiary (FEGLI)</b>	<b>Data Elements in SF-2823 pertain to the Applicant and Beneficiary for the applicant</b>
Applicant Name, Last, first, middle	Applicant Home address	Beneficiary Social Security Number
Applicant Date of Birth	Applicant Civil Service Annuity (CSA), CSI, or Office of Worker Compensation Program (OWCP) claim number	Applicants Beneficiary Address
Applicant Social Security Number	Beneficiary First name, middle initial, and last name of each beneficiary for the applicant	Beneficiary Relationship to applicant
<b><i>Designation of Beneficiary (FERS)</i></b>		
<b><u>SF-3102</u></b>	<b>Designation of Beneficiary (FERS)</b>	<b>Data Elements in SF-3102 pertain to the Applicant and Beneficiary</b>
Applicant Name, Last, First, Middle	Applicant Social Security Number	Applicant Home address
Applicant Date of Birth	Applicant If retired claim number	Applicant Beneficiary First name, initial, and last name of each beneficiary
<b><i>Designation of Beneficiary Unpaid Compensation of Deceased Fed Employee</i></b>		
<b><u>SF-1152</u></b>	<b>Designation of Beneficiary Unpaid Compensation of Deceased Fed Employee</b>	<b>Data Elements in SF-1152 pertain to the Applicant and Beneficiary for the applicant</b>
Applicant Name Last, First, Middle	Applicant Address	Address of each Applicants beneficiary
Applicant Date of birth	Applicants Beneficiary First name, middle initial, and last name of each beneficiary	Beneficiary Relationship to Applicant
Applicant Social Security Number		
<b><i>Thrift Savings Plan Designation of Beneficiary</i></b>		
<b><u>TSP-3</u></b>	<b>Thrift Savings Plan Designation of Beneficiary</b>	<b>Data Elements in TSP-3 pertain to the Applicant and Beneficiary</b>
Applicant Name Last, First, Middle	Applicant Foreign address	Applicant Beneficiary Social security Number or Tax ID
Applicant TSP Account Number	Applicant Benefits Information (including optional benefits selected)	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	Applicant Beneficiary Home address

	Entity or corporation	
Applicant Home address		
Applicant Name Last, First, Middle	Applicant Foreign address	Applicant Beneficiary Social security Number or Tax ID
<b>Employee Election Form</b>		
<b><u>TSP-1</u></b>	<b>Thrift Savings Plan Enrollment</b>	<b>All Data Elements in TSP-1 pertain to the Applicant</b>
Applicant Name Last, First Middle	Address	Social Security Number
Home Phone Number		
<b>TSP Catch-Up Contribution Form</b>		
<b><u>TSP-1-C</u></b>	<b>TSP Catch-Up Contribution</b>	<b>All Data Elements in TSP-1-C pertain to the Applicant</b>
Applicant Name Last, First, Middle	Social Security Number	Phone Number
Address		
<b>Premium Conversion Waiver/Election</b>		
<b><u>DG-60</u></b>	<b>Premium Conversion Waiver/Election Form</b>	<b>All Data Elements in DG-60 pertain to the Applicant</b>
Applicant Last Name, First Name, Middle Initial	Social Security Number	Applicant Last Name, First Name, Middle Initial
<b>Life/Health Insurance/Benefits</b>		
<b><u>SF-2809</u></b>	<b>Employee Health Benefit Election (FEHB)</b>	<b>Data Elements in SF-2809 pertain to the Applicant and Eligible family member/s</b>
Applicant/Enrollee name last, first, middle initial	Applicant Policy number	Eligible family member/s Gender
Applicant Social Security Number	Applicant Email address	Eligible family member/s Address
Applicant Date of Birth	Applicant Phone number	Eligible family member/s Name of other insurance
Applicant Gender	Eligible family member/s Name Last, First, Middle initial	Eligible family member Name of other insurance and Policy Number
Applicant Marital Status	Eligible family member/s Social Security Number	Eligible family member/s Medicare Claim Number
Applicant Home address	Eligible family member/s Date of Birth	Eligible family member/s Email address
Applicant Name of other insurance and Policy Number		
<b>Life Insurance Election (FEGLI)</b>		
<b><u>SF-2817</u></b>	<b>Life Insurance Election (FEGLI)</b>	<b>All Data Elements in SF-2817 pertain to the Applicant</b>
Name last, first, middle	Social Security Number	Telephone number
Date of birth	Office of Worker's Compensation Programs (OWCP)	
<b>Withholding Allowances/Exemption Certificate</b>		
<b><u>W-4</u></b>	<b>Employee Withholding Allowance</b>	<b>All Data Elements in W4 pertain to the Applicant</b>
Name First, Middle initial, Last Name	Home Address	Marital Status
Employee Address		
AD-349	Employee address	All Data Elements in W4 pertain to the Applicant
Name Last, First, Middle	Social Security Number	Employee Home Address
Employee Mailing Address	Signature of Employee	
<b>Employment Eligibility Verification</b>		
<b><u>I-9</u></b>	<b>Employment Eligibility</b>	<b>Not All Data Elements in form</b>

	<b>Verification</b>	<b>pertain to the Applicant</b>
Name Last, First, Middle initial	Other Names Used	Home Address
Date of Birth	Social Security Number	Email Address
Telephone Number	Citizenship Status	Signature of Employee
Signature of Preparer or Translator	Name Last and First of Preparer	Address of Preparer
Identifying Document number	Signature of Employer or Authorized Representative	Title of Employer
Employer's business	Business Address	Date of Rehire
<b><i>Personal Identity Verification for Federal Employees and Contractors</i></b>		
<b>Form 13760</b>	<b>Personal Identity Verification for Federal Employees and Contractors</b>	<b>Not All Data Elements in form pertain to the Applicant</b>
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
<b><i>Certificate of Non-residence in the District of Columbia</i></b>		
<b><u>Form D-4A</u></b>	<b>Certificate of Non-residence in the District of Columbia</b>	<b>Not All Data Elements in form pertain to the Applicant</b>
Name First, Middle Initial, Last Name	Temporary DC address	Social Security Number
Permanent Address	Signature	
<b><i>Notification of Personnel Action</i></b>		
<b><u>SF-50</u></b>	<b>Notification of Personnel Action</b>	<b>Not All Data Elements in form pertain to the Applicant</b>
Name Last, First, Middle	Social Security Number	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	
<b><i>Transfer of Information Between Agencies</i></b>		
<b><u>TSP-19</u></b>	<b>Thrift Savings Plan</b>	<b>Not All Data Elements in form pertain to the Applicant</b>
Name Last, First, Middle	Social Security Number	Date of Birth
Date of Transfer	TSP Status Code	TSP Service Compilation Date
TSP Vesting Code	Contribution Election Information	Catch-up contribution information
Loan information	Loan Account Number and Payment Amount	Employee Nonpay status
Agency Name	Name of Contact Person	Telephone Number of Contact Person
Agency Location		
<b><i>Personnel Public Financial Disclosure Report</i></b>		
<b><u>OGE Form 278e</u></b>	<b>Personnel Public Financial Disclosure Report</b>	<b>Not All Data Elements in form pertain to the Applicant</b>
Name Last, First, Middle Initial	Title of Position	Department or Agency

Location of Present Office	Office Telephone Number	Presidential Nomination Congressional Committee
Certifying Individual's Signature	Reviewer's Signature	Ethics 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
Compensation in Excess of \$5,000 Paid by One Source		
<b><i>Confidential Financial Disclosure Report</i></b>		
<a href="#">OGE Form 450</a>	<b>Confidential Public Financial Disclosure Report</b>	<b>Not All Data Elements in form pertain to the Applicant</b>
Name Last, First, Middle Initial	Position/Title	Agency
Branch/Unit and Address	Work Number	E-mail 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
<b><i>US Department of State Foreign Service Designation of Beneficiary</i></b>		
<a href="#">DS-5002</a>	<b>Designation of Beneficiary</b>	<b>Data Elements in DS-5002 pertain to Applicant and Designation for beneficiary or beneficiaries</b>
Applicant Name Last, First, Middle	Applicant Post of Assignment	Address of each beneficiary
Applicant Date of Birth	Applicant Address	Relationship to applicant
Applicant Social Security Number	Applicants Designation for beneficiary or beneficiaries First name, middle initial, and last name of each beneficiary	

### **Section 4.3: Sources of information and the method and manner of collection**

*Applicants who receive and accept job offers for employment with a Federal agency that is serviced by HR Connect, 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 Entry on Duty System (EODS), these forms are completed within EODS and the necessary information sent to HR Connect via an interface.*

### **Section 4.4: Privacy and/or civil liberties risks related to collection**

#### **Notice of Authority, Principal Uses, Routine Uses, and Effect of not Providing Information**

When Federal agencies use a form to obtain 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 her/him, if any, of not providing all or any part of the requested information.” 5 U.S.C § 522a(e)(3).

**Section 4.4(a)**  Yes  No Is any of the [PII](#) maintained in the system or by the project collected directly from an individual?

**Section 4.4(b)**  Yes  No  N/A Was the information collected from the individual using a form (paper or electronic)?

**Section 4.4(c)**  Yes  No  N/A If the answer to Section 4.4(b) was “yes,” was the individual notified (on the form in which the [PII](#) was collected or on a separate form that can be retained by the individual) about the following at the point where the information was collected (e.g., in a form; on a website).

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

*The authority, principal purpose(s), and routine uses of information collected have been communicated to the provider in the form or on the website at the point of collection*

## Use of Social Security Numbers

Social Security numbers (“SSN”) are commonly used by identity thieves to commit fraudulent acts against individuals. The SSN is one data element that has the ability to harm the individual and requires more protection when used. Therefore, in an effort to reduce risk to individuals and federal agencies, OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, (May 22, 2007) required agencies to reduce the use of SSNs in agency systems and programs and to identify instances in which the collection is superfluous. In addition, OMB mandated agencies to explore alternatives to agency use of SSNs as personal identifiers for Federal employees and members of the public.

In addition, 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 4.4(d)**  Yes  No  N/A Does the system or project maintain SSNs?

**Section 4.4(e)**  Yes  No  N/A Are there any alternatives to the SSNs as a personal identifier? If yes, please provide a narrative explaining why other alternatives to identify individuals will not be used.



**Section 4.4(f)**  Yes  No  N/A Will individuals be denied any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN? If yes, please check the applicable box:

- SSN disclosure is required by Federal statute or Executive Order. ; or
- the SSN is disclosed to any Federal, state, or local agency maintaining a [system of records](#) 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. *If checked, please provide the name of the system of records in the space provided below.*

**Section 4.4 (g)**  Yes  No  N/A When the SSN is collected, are individuals given notice whether disclosure is mandatory or voluntary, the legal authority such number is solicited, and what uses will be made of it? If yes, please explain what means are used to provide notice.

*The SSN is required by HR Connect's payroll provider, the United States Department of Agriculture, National Finance Center (NFC). NFC has operated as a payroll system of records since 1973.*

### First Amendment Activities

The [Privacy Act](#) provides 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).

**Section 4.4(h)**  Yes  No Does the system or project maintain any information describing how an individual exercises their rights guaranteed by the First Amendment?

**Section 4.4(h)** If the system or project maintains information describing how an individual exercises their rights guaranteed by the First Amendment, do any of the following exceptions apply (the information may be maintained if any of the exceptions apply)?

N/A (system or project does not maintain any information describing how an individual exercises their rights guaranteed by the First Amendment so no exceptions are needed)

- The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.
- The information maintained is pertinent to and within the scope of an authorized law enforcement activity.
- There is a statute that expressly authorizes its collection.

*information*

*HR Connect does not collect information about first amendment activities.*

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

The following sections require a clear description of the system's or project's use of information.

### Section 5.1: Describe how and why the system or project uses the information it collects and maintains

Please describe all of the uses of the information types and groupings collected and maintained by the system or project (see [Section 4.2](#)), including a discussion of why the information is used for this purpose and how it relates to the mission of the bureau or office that owns the system.

The information collected and maintained in the system is used by Treasury and other federal agencies to:

- (1) record deductions, leave accrued and taken ; maintain and display Leave and Earnings statements; commence and terminate allotments; answer inquiries; and process claims;
- (2) maintain current and historical personnel records and prepare individual administrative transactions relating to education and training; job assignment; career development; evaluation; promotion, compensation, separation and retirement;
- (3) provide data for the production of reports, statistical surveys, rosters, documentation, and studies required for orderly personnel administration within Treasury;
- (4) maintain and administer organizational setup, such as organizational hierarchy; reporting hierarchy; job codes and classification; pay plans and associated salary (including locality pay); work locations; and position budget management;
- (5) perform personnel functions for Federal agencies for which Treasury is a cross-services provider and provide information necessary to enable the payroll provider, National Finance Center (NFC), to perform the activities necessary to calculate and distribute pay.

[PII](#) is used to identify employees for the purpose of carrying out the system objectives, as described above. Other uses are discussed in Section 5.4, Information sharing with external agencies.

### Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them

The [Privacy Act](#) requires that Federal agencies “collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs.” 5 U.S.C. § 552a(e)(2).

**Section 5.1(a)**  Yes  No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination about an individual’s rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

**Section 5.1(b)**  Yes  No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual’s rights, benefits, and privileges under federal programs?

**Section 5.1(c)**  Yes  No  N/A If information could potentially be used to make an adverse determination about an individual’s rights, benefits, and privileges under federal programs, does the system or project collect information (to the greatest extent practicable) directly from the individual?

*The vast majority of information maintained in the system is collected directly from the employee. Such information could be used to make an adverse determination about an individual’s rights, benefits, and privileges under federal programs. Agencies with which HR Connect shares information pursuant to the routine uses in the applicable systems of records notices (see below) may also use information from the system to make adverse decisions.*

*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. This is enforced by the*

payroll provider system, NFC. The overall rating is not determined by HR Connect; 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. HR Connect maintains the overall rating and the performance award amount and electronically transmits both to the payroll provider, NFC. HR Connect does not make any determinations about the award amount.

## Data Mining

As required by Section 804 of the [Implementing the 9/11 Commission Recommendations 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 reports available at: <http://www.treasury.gov/privacy/annual-reports>.

**Section 5.1(d)**  Yes  No Is information maintained in the system or by the project used to conduct “data-mining” activities as that term is defined in the [Implementing the 9-11 Commission Act](#)?

*No privacy and civil liberties risks were identified.*

## [Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared](#)

### Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

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 2 above), an agency may exempt the [system of records](#) (or a portion of the records) from this requirement.

**Section 5.2(a)**  Yes  No Is all or any portion of the information maintained in the system or by the project: (a) part of a [system of records](#) and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the [Privacy Act](#)?

*None of the information maintained in the system is both part of a system of records and exempt from the accuracy, relevance, timeliness, and completeness requirements of the Privacy Act.*

## Computer Matching

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

Pursuant to the [Privacy Act](#), as amended, 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 and recipient agencies. The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

<p><a href="#">Section 5.2(b)</a> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Is any of the information maintained in the system or by the project (a) part of a <a href="#">system of records</a> and (b) used as part of a matching program?</p> <p><a href="#">Section 5.2(c)</a> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> N/A Is there a matching agreement in place that contains the information required by Section (o) of the <a href="#">Privacy Act</a>?</p> <p><a href="#">Section 5.2(d)</a> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A Are assessments made regarding the accuracy of the records that will be used in the matching program?</p> <p><a href="#">Section 5.2(e)</a> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A Does the bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings, or obtain Data Integrity Board approval in accordance with Section (p) of the <a href="#">Privacy Act</a> before taking adverse action against the individual?</p>
<p><i>There are no matching agreements in place between HR Connect and any other system of record.</i></p>

### Ensuring Fairness in Making Adverse Determinations About Individuals

Federal agencies are required to “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). This requirement also applies when merging records from two or more sources where the merged records are used by the agency to make any determination about any individual.

<p><a href="#">Section 5.2(f)</a> <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No With respect to the information maintained in the system or by the project, are steps taken to ensure all information used to make a determination about an individual is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?</p>
<p><i>The collected data is verified for accuracy, relevancy, and completeness by the employees who submit their information to Treasury and other federal agencies that use HR Connect. The information is also reviewed by participating agencies' HR Specialists and undergoes the quality assurance process put in place by each agency.</i></p>

### Merging Information About Individuals

<p><a href="#">Section 5.2(g)</a> <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Is information maintained in the system or by the project merged with electronic or non-electronic information from internal or external sources (e.g., other files or systems)?</p> <p><a href="#">Section 5.2(h)</a> <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Once merged, is the information used in making determinations about</p>
---

individuals (e.g., decisions about whether the individual will receive a financial benefit or payment, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)?

[Section 5.2\(i\)](#)  Yes  No  N/A Are there documented policies or procedures for how information is merged?

[Section 5.2\(j\)](#)  Yes  No  N/A Do the documented policies or procedures address how to proceed when partial matches (where some, but not all of the information being merged matches a particular individual) are discovered after the information is merged?

[Section 5.2\(k\)](#)  Yes  No  N/A If information maintained in the system or by the project is used to make a determination about an individual, are steps taken to ensure the accuracy, relevance, timeliness, and completeness of the information as is reasonably necessary to assure fairness to the individual?

*Information sent to HR Connect pertaining to individuals must include a unique identifier in a format recognized by HR Connect. This unique identifier is used to merge information. If the unique identifier is not in HR Connect or if there is only a partial match between the unique identifier and other identifying information and the nature of action code does not support this partial match, then the information associated with that unique identifier is sent to an error file, which is subsequently returned to the sender for resolution.*

## Policies and Standard Operating Procedures or Technical Solutions Designed to Ensure Information Accuracy, Completeness, and Timeliness

[Section 5.2\(l\)](#)  Yes  No  N/A If information maintained in the system or by the project is used to make any determination about an individual (even if it is an exempt [system of records](#)), are there documented policies or standard operating procedures for the system or project that address the accuracy, completeness, and timeliness of the information?:

[Section 5.2\(m\)](#)  Yes  No Does the system or project use any software or other technical solutions designed to improve the accuracy, completeness, and timeliness of the information used to make an adverse determination about an individual's rights, benefits, and/or privileges (regardless of if it is an exempt [system of records](#))?

*The system's paperless personnel actions electronically route actions for approval, greatly reducing processing time and the human error associated with manual processing.*

## Accuracy, Completeness, and Timeliness of Information Received from the Source

[Section 5.2\(n\)](#)  Yes  No Did Treasury or the bureau receive any guarantee, assurance, or other information from any information source(s) regarding the accuracy, timeliness and completeness of the information maintained in the system or by the project?

*Each agency/customer that uses HR Connect is responsible for the integrity/quality of the data entered into the system, including accuracy, completeness, and timeliness of the information. The information in the system is also derived directly from the individual, thereby generally providing a higher assurance of its accuracy. Treasury and the agency/customers who use HR Connect do not, however, receive any guarantees about the quality of the information. If errors are discovered, they are corrected.*

## Disseminating Notice of Corrections of or Amendments to PII

[Section 5.2\(o\)](#)  Yes  No  N/A Where feasible and appropriate, is there a process in place for disseminating corrections of or amendments to the [PII](#) maintained in the system or by the project to all internal and external information-sharing partners?

[Section 5.2\(p\)](#)  Yes  No  N/A Where feasible and appropriate, does the process for disseminating corrections or amendments include notifying the individual whose information is corrected or amended?

*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 HR Connect, functionality can be enabled for contractors to update/correct their own information directly in HR Connect.

### **Section 5.3: Information sharing within the Department of the Treasury**

#### **Internal Information Sharing**

**Section 5.3(a)**  Yes  No Is **PII** maintained in the system or by the project shared with other Treasury bureaus?

**Section 5.3(b)**  Yes  No  N/A Does the Treasury bureau or office that receives the **PII** limit access to those Treasury officers and employees who have a need for the **PII** in the performance of their official duties (i.e., those who have a “need to know”)?

*Data in the system can only be accessed by customer agency employees and managers , the customer’s servicing human resources agency (if they have one) as well as HR Connect staff who administer the system databases, code, functionality, and customer support. Each individual’s access is based on the permissions in their system profile. Customer agencies and support organizations within the Department of the Treasury include:*

- Alcohol and Tobacco Tax and Trade Bureau (TTB)
- Bureau of Engraving and Printing (BEP)
- Departmental Offices (DO)
- Financial Crimes Enforcement Network (FinCEN)
- Internal Revenue Service (IRS)
- Office of the Comptroller of the Currency (OCC)
- Office of Fiscal Service (FS)
- Office of the Inspector General (OIG)
- Office of Thrift Supervision
- Special Inspector General for the Troubled Asset Relief Program (SIGTARP)
- Treasury Inspector General for Tax Administration (TIGTA)
- Treasury Office of the Inspector General
- United States Mint

#### **Memorandum of Understanding/Other Agreements Limiting Treasury’s Internal Use/Disclosure of PII**

**Section 5.3(c)**  Yes  No  N/A Is any of the **PII** maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency that provided the information to the Treasury or subject to an international agreement or treaty) that limits or places conditions on Treasury’s internal use, maintenance, handling, or disclosure of the **PII**?

*Treasury uses the PII in the system for the sole purpose of human resources administration and payroll. The PII that is necessary for employees to receive a paycheck is sent to the payroll services provider, the United States Department of Agriculture, National Finance Center (NFC).*

#### **Internal Information Sharing Chart**

Internal HRC customers access their own information directly in HR Connect. Therefore, no internal sharing is necessary.

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

#### **External Information Sharing**

**Section 5.4(a)**  Yes  No Is **PII** maintained in the system or by the project shared with agencies,

organizations, or individuals external to Treasury?

Data in the system can only be accessed by customer agency employees and managers, the customer's servicing human resources agency (if they have one) as well as HR Connect staff who administer the system databases, code, functionality, customer support, and the payroll provider. Each individual's access is based on the permissions in their system profile. Customer agencies and support organizations outside of the Department of the Treasury include:

- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATFE)
- Consumer Financial Protection Bureau (CFPB)
- Department of Commerce (DOC)
- Department of Labor (DOL)
- General Services Administration (GSA)
- Government Accountability Office (GAO)
- Housing and Urban Development (HUD)
- National Finance Center (NFC)
- SuccessFactors
- United States Agency for International Development (USAID)
- United States Secret Service (USSS)
- United States Office of Personnel Management

## Accounting of Disclosures

**Section 5.4(b)**  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), do you maintain a paper or electronic log or other record of 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? See 5 U.S.C § 552a(c).

**Section 5.4(c)**  Yes  No  N/A If you do not keep a running tabulation of every disclosure at the time it is made, are you able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to [Privacy Act](#) requests in a timely fashion?

**Section 5.4(d)**  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), do you retain the log or other record of the date, nature, and purpose of each disclosure, for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made? ,

**Section 5.4(e)**  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), does your bureau or office exempt the [system of records](#) (as allowed by the [Privacy Act](#) in certain circumstances) from the requirement to make the accounting available to the individual named in the record?

**Section 5.4(f)**  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), does your bureau or office exempt the [system of records](#) (as allowed by the [Privacy](#)

<p><a href="#">Act</a> in certain circumstances) from the requirement to inform any person or other agency about any correction or notation of dispute made by the agency of any <a href="#">record</a> that has been disclosed to the person or agency if an accounting of the disclosure was made?</p>	
<p><i>HR Connect customers are the information owners of their data in the system. Disclosures of PII to non-customer agencies are tracked via electronic logs, which are retained for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made.</i></p>	

**Statutory or Regulatory Restrictions on Disclosure**

**Section 5.4(g)**  Yes  No In addition to the [Privacy Act](#), are there any other statutory or regulatory restrictions on the sharing of any of the PII maintained in the system or by the project (e.g., 26 U.S.C § 6103 for tax returns and return information)?

**Memorandum of Understanding Related to External Sharing**

**Section 5.4(h)**  Yes  No  N/A Has Treasury (including bureaus and offices) executed a Memorandum of Understanding, or entered into any other type of agreement, with any external agencies, organizations, or individuals with which/whom it shares [PII](#) maintained in the system or by the project?

*Treasury is a cross-services provider to the other Federal agencies listed in Section 5.4(a) 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. As the Servicing Agency, Treasury provides data to the third-party application administrators listed in Section 5.4(a). There are agreements signed between Treasury and these third-party application administrators.*

**Memorandum of Understanding Limiting Treasury’s Use or Disclosure of PII**

**Section 5.4(i)**  Yes  No Is any of the [PII](#) maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency, an international agreement or treaty, or contract with private vendor that provided the information to Treasury or one of its bureaus) that limits or places conditions on Treasury’s internal use or external (i.e., outside Treasury) sharing of the [PII](#)?

*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 in Section 5.4(a). There are agreements signed between Treasury and these third-party application administrators.*

**Memorandum of Understanding Limiting External Party’s Use or Disclosure of PII**

**Section 5.4(j)**  Yes  No Is any of the [PII](#) maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party’s use, maintenance, handling, or disclosure of [PII](#) shared by Treasury?

*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 in Section 5.4(a). There are agreements signed between Treasury and*



these third-party application administrators.

### External Information Sharing Chart 1

<u>Section 5.4(k)</u> <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Is information from the system or project shared externally?			
<b>External Recipient's Name</b>	Department of Agriculture, NFC	To on site contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Department of the Treasury.	To other Federal agencies and vendors with whom the Department has entered into a cross servicing agreement that provides for the delivery of automated human resources operations.
Purpose of the Sharing PII Shared	To provide all services related to processing payroll transactions applicable to the National Finance Center's Payroll/Personnel System (PPS).	When necessary to accomplish an agency function.	For the delivery of automated human resources operations. These operations may include maintaining current and historical payroll and personnel records, and providing reports, statistical surveys, rosters, documentation, and studies as required by the other federal agency to support its personnel administration activities.
Content of Applicable Routine Use/Citation to the <a href="#">SORN</a>	See above.	See above.	See above.
Applicable Statutory or Regulatory or Restrictions on Information Shared	Economy Act (31 U.S.C. 1535/FAR 17.5)	The Privacy Act of 1974.	The Privacy Act of 1974.
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Source/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of <a href="#">PII</a> )	Interagency Agreement (IAA) Number NFC-16-9101 Service Level Agreement Payroll/Processing System	Enterprise Business Solutions/HR Connect (EBS HRC) Agreement to Safeguard Sensitive Data form	The interagency agreement number relative to the particular cross-servicing agreement
Method(s) Used to Transfer <a href="#">PII</a> (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other)	Electronic file feed, IPsec VPN tunnel	Direct login to a non-production HR Connect environment	Electronic file feed, IPsec VPN tunnel

*<< Space for Narrative Explanation of the Answer to Section 5.4(k) Privacy and/or civil liberties*

risks presented and mitigation efforts >>

### Obtaining Consent Prior to New Disclosures Not Included in the SORN or Authorized by the Privacy Act

**Section 5.4(l)**  Yes  No  N/A Is the individual's consent obtained, where feasible and appropriate, prior to any **new** disclosures of previously collected records in a [system of records](#) (those not expressly authorized by the [Privacy Act](#) or contained in the published [SORN](#) (e.g., in the routine uses))?

*There are no disclosures of previously collected records in the system of records not expressly authorized by the Privacy Act or contained in the published SORN.*

## [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: Privacy Act System of Records Notice \(SORN\)](#)

For collections of [PII](#) that meet certain requirements, the [Privacy Act](#) requires that the agency publish a [SORN](#) in the *Federal Register*.

#### System of Records

**Section 6.1(a)**  Yes  No Does the system or project retrieve [records](#) about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? (see items selected in [Section 4.2](#) above)

**Section 6.1(b)**  Yes  No  N/A Was a [SORN](#) published in the *Federal Register* for this [system of records](#)?

*Data is retrievable by personal identifier. Data can be retrieved either by the employee identifier, as it pertains to an individual, or by the name of the employee, if the information is being retrieved by either the manager of record or (in the case of contractors/consultants) by the manager of the contract.*

*The System of Record Notice is Treasury .001 – Treasury Personnel and Payroll System.*

### [Section 6.2: 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 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).

#### Paperwork Reduction Act Compliance

**Section 6.2(a)**  Yes  No Does the system or project maintain information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government)?

**Section 6.2(b)**  Yes  No  N/A Does the project or system involve a new collection of [information in identifiable form](#) for 10 or more persons from outside the federal government?

**Section 6.2(c)**  Yes  No  N/A Did the project or system complete an Information Collection Request (“ICR”) and receive OMB approval?

*While there is information for more than 10 individuals maintained within HR Connect, the information request referenced in 6.2(b) was done one person at a time.*

### **Section 6.3: 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 [NARA](#) for permanent retention upon expiration of this period.

#### **NARA Records Retention Requirements**

**Section 6.3(a)**  Yes  No Are the records used in the system or by the project covered by NARA’s General Records Schedules (“GRS”) or Treasury/bureau Specific Records Schedule (SRS)?

**Section 6.3(b)**  Yes  No Did NARA approved a retention schedule for the records maintained in the system or by the project?

**Section 6.3(c)**  Yes  No  N/A If NARA did not approve a retention schedule for the records maintained in the system or by the project and the records are not covered by NARA’s GRS or Treasury/bureau SRS, has a draft retention schedule (approved by all applicable Treasury and/or Bureau officials) been developed for the records used in this project or system?

*The retention periods of data contained in this system are covered by General Records Schedules #1, Civilian Personnel Records, and have various retention periods for specific types of data. Reports in the system are retained for 7-14 days, based on data management business rules. The procedures for eliminating the data at the end of the retention period adhere to the Federal Records Act of 1950 and National Archives and Records Administration guidelines, in addition to the Treasury Information Systems Life Cycle (ISLC) management requirements.*

### **Section 6.4: 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”). Different security requirements apply to National Security Systems.

#### **Federal Information System Subject to FISMA Security Assessment and Authorization**

**Section 6.4(a)**  Yes  No  N/A Is the system a federal [information system](#) subject to FISMA requirements?

**Section 6.4(b)**  Yes  No  N/A Has the system or project undergone a SA&A and received ATO?  
*or civil liberties issues were identified.*

#### **Access Controls and Security Requirements**

**Section 6.4(c)**  Yes  No Does the system or project include access controls to ensure limited access to information maintained by the system or project?

*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.*

### Security Risks in Manner of Collection

**Section 6.4(d)**  Yes  No In [Section 4.3](#) above, you identified the sources for information used in the system or project and the method and manner of collection. Were any security, privacy, or civil liberties risks identified with respect to the manner in which the information is collected from the source(s)?

*There were no security, privacy, or civil liberties risks identified with respect to the manner in which the information is collected from the source(s).*

### Security Controls When Sharing Internally or Externally

**Section 6.4(e)**  Yes  No  N/A Are all Treasury/bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system 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 unique user credentials. 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, HR Connect Program Office. The companies must then adhere to the prescribed configuration management principles and procedures in conjunction with the HR Connect Program Office information systems protocols to set up a periodic file feed with the extracted information. In support of the HSPD-12 Initiative, HR Connect has implemented Web Services to provide data exchange services with Treasury Debt Management Services (DMS).*

### Monitoring of Individuals

**Section 6.4(f)**  Yes  No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?

*HR Connect does provide the capability to identify an employee via the employee identifier to gain access to the system through the network gateway. It also provides the capability to locate and authenticate an individual to ensure that only authorized individuals are utilizing the system. The monitoring capabilities are a security requirement in order to ascertain whether or not an individual is attempting to thwart the security mechanisms, manipulate data that is not owned by the individual, or access permissions under other than 'need-to-know' principles.*

### Audit Trails

**Section 6.4(g)**  Yes  No Are audit trails regularly reviewed for appropriate use, handling, and disclosure of PII maintained in the system or by the project inside or outside of the Department?

*HR Connect has extensive auditing capabilities turned on in the system. Agencies have the ability to review auditing trails related to their own data, either by using the appropriate roles and permissions to access this information or contacting the HR Connect Help Desk for assistance in accessing this information. Each agency is responsible for establishing its own regular review of audit trails, as appropriate.*

## [Section 6.5: 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.

### Applicability of and Compliance With the Rehabilitation Act

**Section 6.5(a)**  Yes  No Will the project or system 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)?  
*The Rehabilitation Act is not applicable*

**Section 6.5(b)**  Yes  No  N/A Does the system or project comply 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?

*HR Connect is based on a COTS product (Oracle PeopleSoft). The COTS product platform for HR Connect 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.*

*Oracle uses the VPAT to represent the degree of conformance to various accessibility standards and guidelines, including Section 508 (as released in 2001), WCAG 1.0, and WCAG 2.0. Depending on when a product was developed and released, different standards may be listed. Oracle is an active member on the ITI group that is working to enhance the VPAT to address future standards.<sup>1</sup>*

*The VPAT for PeopleSoft Enterprise PeopleTools 8.54, the current version of the application's foundational software, can be viewed at <http://www.oracle.com/us/corporate/accessibility/templates/t2-4023.html>*

*The analysis of the HR Connect application to identify the areas of non-compliance with 508 is expected to begin in Q2FY17. Once all gaps are identified, a plan will be developed for closing the gaps and bringing the system into full compliance. At that time, a mitigation strategy will be developed for any anticipated areas of non-compliance that persist.*

<sup>1</sup> <http://www.oracle.com/us/corporate/accessibility/vpats/index.html>

## Section 7: Redress

### Access Under the Freedom of Information Act and Privacy Act

**Section 7.0(a)**  Yes  No Does the agency have a published process in place by which individuals may seek records under the [Freedom of Information Act](#) and [Privacy Act](#)?

*The Treasury/bureaus FOIA and PA disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C.*

### Privacy Act Access Exemption

**Section 7.0(b)**  Yes  No Was any of the information that is maintained in [system of records](#) and used in the system or project exempted from the access provisions of the [Privacy Act](#)?

*The system is not exempt from the access provisions of the Privacy Act.*

### Additional Redress Mechanisms

**Section 7.0(c)**  Yes  No With respect to information maintained by the project or system (whether or not it is covered by the [Privacy Act](#)), does the bureau or office that owns the project or system have any additional

mechanisms other than [Privacy Act](#) and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

*The HR Connect system permits the individual to update their data throughout their employment to keep it current. The information maintained in the system may not be used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs.*