



Privacy and Civil Liberties Impact Assessment
for

CareerConnector

April 16, 2020

Reviewing Official

Timothy H. Skinner

Bureau Privacy and Civil Liberties Officer

Departmental Offices

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 is an update to a preexisting PCLIA for this system.

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 limit 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 PCLIAAs 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

Monster Government Solutions (Monster) is a Software as a Service (SaaS) provider that developed a web-based system which provides federal agency customers with online services that automate federal recruitment and staffing activities. The Monster Hiring Management Enterprise software provides a service delivery mechanism that allows Treasury and its customers to use the public internet to conduct recruitment and staffing activities. Treasury rebrands the Monster Hiring Management Enterprise under the name “CareerConnector.”

CareerConnector facilitates recruitment and staffing efforts by classifying positions, posting and managing vacancies, collecting and processing applications, rating and ranking applicants, making selections, onboarding new hires, and managing the collection and submission of information through a Recommendation portal, which provides a secure way for references to submit feedback and/or

provide a letter of recommendation to the hiring authority through the system. The onboarding of new hires may require applicants to submit additional personal information in order to initiate and complete the entrance on duty process.

Most Treasury bureaus perform entrance on duty functions through a different information system called the Entrance on Duty System (EODS). The EODS is a two-component, web-based Human Resource (HR) product that facilitates the completion of new hire forms via an automated online process as a part of the HR Connect Line of Business. EODS maintains its own Privacy and Civil Liberties Impact Assessment. The Internal Revenue Service (IRS) does not use EODS. It uses CareerConnector for recruiting and to onboard new employees.

CareerConnector also provides email correspondence functionality that allows Treasury to notify employment candidates regarding hiring decisions for particular positions. The system also provides a comprehensive analytics reporting tool that generates data that can be used to help drive strategic hiring decisions.

CareerConnector receives applicant profile information, resume and supporting documentation from USAJOBS which is tied to the applicant as they complete the application process in CareerConnector. USAJOBS is the federal government's official employment site. It helps human resources (HR) professionals recruit, retain, and honor the federal government's workforce. Federal HR professionals can send job vacancy announcements to the USAJOBS internet site for public notification. Applicants sign in to the USAJOBS website to begin the application process. Applicants' information received from USAJOBS is used by HR to determine eligibility and qualifications in order for hiring managers to make selections.

Information stored and processed by CareerConnector includes employment-related data such as job vacancies, position descriptions, position requirements, qualifications, applicant questions, and various other data related to hiring decisions and onboarding. CareerConnector also stores applicant information such as social security numbers and professional resumes which may contain employment history, personal address, phone number, email, and educational history.

Some information collected and stored in CareerConnector is shared with Treasury's primary HR system, HR Connect. HRConnect supports the human resources functions for the Department of the Treasury and other federal agencies that use HRConnect as part of a cross services initiative to reduce federal government expenditures. Information is also shared with Treasury's Enterprise Data Management system which provides data collection and analysis to aid with recruitment and hiring planning and strategy. For applicants who complete third-party assessment tests through the Performance Assessment Network (PAN) as part of the application process, scores from PAN are imported to CareerConnector. The table below summarizes the list of the forms contained in CareerConnector:

Form ID	Form Name
DD-214	The Report of Separation
SF-15 relatives	Application for 10-Point Veteran Preference (to be used by veterans and of veterans)
OF-306	Declaration for Federal Employment
SF-61	Appointment Affidavit
SF-144	Statement of Prior Federal Service
SF-181	Ethnicity and Race Identification
SF-256	Self-Identification of Disability
INS-9	Immigration & Naturalization Service Employment Eligibility Verification
SF-312	Classified Information Non-Disclosure Agreement
SF-1199A	Direct Deposit Sign-Up
FMS-2231	Fast Start Direct Deposit
SF-3109	FERS Election of Coverage
SF-2808	Designation of Beneficiary (CSRS)
SF-2823	Designation of Beneficiary (FEGLI)
SF-3102	Designation of Beneficiary (FERS)
SF-1152	Designation of Beneficiary Unpaid Compensation of Deceased Fed Employee
TSP-3	Thrift Savings Plan Designation of Beneficiary
TSP-1	Thrift Savings Plan Enrollment
TSP-1-C	TSP Catch-Up Contribution
DG-60	Premium Conversion Waiver/Election Form

Form ID	Form Name
SF-2809	Employee Health Benefit Election (FEHB)
SF-2817	Life Insurance Election (FEGLI)
W-4	Employee Withholding Allowance
I-9	Employment Eligibility Verification
Form 13760	Personal Identity Verification for Federal Employees and Contractors
Form D-4A	Certificate of Non-residence in the District of Columbia
SF-50	Notification of Personnel Action
TSP-19	Thrift Savings Plan
OGE Form 278e	Personnel Public Financial Disclosure Report
OGE Form 450	Confidential Public Financial Disclosure Report
DS-5002	Designation of Beneficiary
IRS Form 12114 (OMB 1545-1921)	OF-306 Continuation Sheet
IRS Form 12325	Military Status
IRS Form 12333	Consent for Fingerprint Check
IRS Form 12854 (OMB 1545-1919)	Government Service Information
IRS Form 11340	Disclosure and Authorization Pertaining to Consumer Reports pursuant to the Fair Credit Reporting Act (FCRA)
IRS Form 12311 (OMB 1545-1920)	Repayment of a Federal Government Buyout and Possible Suspension of Severance Pay
IRS Form 11340	Information Provided Concerning the Disclosure and Authorization Pertaining to Consumer Reports pursuant to the Fair Credit Reporting Act (FCRA)
SF-180	Request Pertaining to Military Records

List of Treasury CareerConnector Customers:

Non Treasury Customers

- *Department of Commerce*
- *United States Agency for International Development*
- *Federal Communications Commission*
- *Government Accountability Office*
- *Peace Corps*

Non-Treasury Customers Serviced by Bureau of Fiscal Service (BFS)-Administrative Resource Center (ARC)

- *Armed Forces Retirement Home*
- *Consumer Financial Protection Bureau*
- *Federal Housing Finance Agency Office of Inspector General*
- *United States Department of Housing and Urban Development*
- *Denali Commission*
- *Federal Mine Safety and Health Review Commission*
- *Office of Government Ethics (OGE)*
- *Department of Veterans Affairs, Office of Inspector General*
- *US Department of Agriculture - Client Experience Center/Office of the Chief Information Officer*
- *Department of Commerce Office of Inspector General*
- *Gulf Coast Ecosystem Restoration Council*

The CareerConnector Program Team works with the vendor to ensure all system functionality works as expected to support recruitment processes, data collection and reporting, as well as continuity of data feeds between all systems. Treasury escalates to the vendor any CareerConnector security, privacy, or technical issues encountered to ensure resolution according to established Service Level Agreements.

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 for the Secretary establishes the mission of the Department of Treasury.
- e-Government Act of 2002 (H.R. 2458/S.803) supports government to government services.
Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons dated November 22, 1943.
- 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:

1. None of the [PII](#) maintained in the system or by the project is part of a [Privacy Act system of records](#);
2. 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;
3. 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;
4. 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 requirement, is there a process to continuously reevaluate and ensure that the [PII](#) remains relevant and necessary?

CareerConnector also stores information collected using the forms listed in the table above (Section 3.1) which are subject to the Paperwork Reduction Act (PRA). Forms that are subject to the PRA must be approved by the OMB Director 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 collect that information. Treasury and OMB have determined that all information collected in CareerConnector using the forms listed in Section 3.1 is relevant and necessary. Treasury will continue to monitor the information collected in these forms and other information collected in CareerConnector to ensure that it remains relevant and necessary.

Section 4.2: PII and/or information types or groupings

To perform their 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 3.3](#) – Authority to Collect.

Only the Internal Revenue Service utilizes the CareerConnector onboarding function to process tentative job offers and conduct initial pre-screening for selectees and to process final job offers for new hires. This may include the collection of the following personally identifiable information (PII) collected in resumes or forms: identifying numbers, medical/emergency contact information, biometrics/distinguishing features/characteristics of individuals, and specific information/file types.

Biographical/General Information		
<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 checked="" type="checkbox"/> Alias (including nickname)
<input checked="" 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 checked="" type="checkbox"/> Nationality	<input type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Business e-mail address	<input checked="" type="checkbox"/> Country of Birth	<input checked="" type="checkbox"/> Spouse Information
<input checked="" type="checkbox"/> Personal Financial Information (including loan information)	<input checked="" type="checkbox"/> City or County of Birth (does this apply to US only?)	<input checked="" type="checkbox"/> Children Information
<input type="checkbox"/> Business Financial Information (including loan information)	<input checked="" type="checkbox"/> Immigration Status	<input checked="" type="checkbox"/> Information about other relatives.
<input checked="" type="checkbox"/> Marital Status	<input checked="" type="checkbox"/> Citizenship	<input checked="" type="checkbox"/> Professional/personal references or other information about an individual's friends, associates or acquaintances.
<input type="checkbox"/> Religion/Religious Preference	<input type="checkbox"/> Device settings or preferences (e.g., security level, sharing options, ringtones).	<input type="checkbox"/> Global Positioning System (GPS)/Location Data
<input type="checkbox"/> Sexual Orientation	<input type="checkbox"/> User names, avatars, etc.	<input type="checkbox"/> Secure Digital (SD) Card or Other Data stored on a card or other technology
<input type="checkbox"/> Cell tower records (e.g., logs, user location, time etc.)	<input type="checkbox"/> Network communications data	<input type="checkbox"/> Cubical or office number
<input type="checkbox"/> Contact lists and directories (known to contain personal information)	<input type="checkbox"/> Contact lists and directories (not known to contain personal information, but uncertain)	<input type="checkbox"/> Contact lists and directories (known to contain only business information)

<input checked="" type="checkbox"/> Education Information	<input checked="" type="checkbox"/> Resume or curriculum vitae	<input checked="" type="checkbox"/> Other (please describe): <i>Performance Reviews; Writing Samples; Cover Letter; Executive Core Qualifications; Selective Service Registration Card, and other position specific information required to assess suitability, assessments results</i>
<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):

Identifying Numbers	
<input checked="" type="checkbox"/> Full Social Security number	<input checked="" type="checkbox"/> Health Plan Beneficiary Number
<input checked="" type="checkbox"/> Truncated/Partial Social Security number (e.g., last 4 digits)	<input checked="" type="checkbox"/> Alien Registration Number
<input type="checkbox"/> Personal Taxpayer Identification Number	<input type="checkbox"/> Business Taxpayer Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Credit Card Number	<input type="checkbox"/> Business Credit Card Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Vehicle Identification Number	<input type="checkbox"/> Business Vehicle Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal License Plate Number	<input type="checkbox"/> Business License Plate Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> File/Case ID Number (individual)	<input type="checkbox"/> File/Case ID Number (business) (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input checked="" type="checkbox"/> Personal Professional License Number	<input checked="" type="checkbox"/> Business Professional License Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Employee Identification Number	<input type="checkbox"/> Patient ID Number
<input type="checkbox"/> Business Bank Account Number	<input checked="" type="checkbox"/> Personal Bank Account Number
<input type="checkbox"/> Commercially obtained internet navigation/purchasing habits of individuals	<input type="checkbox"/> Government obtained internet navigation/purchasing habits of individuals
<input type="checkbox"/> Business License Plate Number (non-sole-proprietor)	<input checked="" type="checkbox"/> Driver's License Number
<input type="checkbox"/> Personal device identifiers or serial numbers	<input checked="" type="checkbox"/> Other Identifying Numbers (please describe): <i>Position Number</i>
<input checked="" type="checkbox"/> 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)	<input type="checkbox"/> Other Identifying Numbers (please describe): _____

Medical/Emergency Information Regarding Individuals		
<input checked="" type="checkbox"/> Medical/Health Information	<input type="checkbox"/> Worker's Compensation Act Information	<input type="checkbox"/> Patient ID Number
<input checked="" type="checkbox"/> Mental Health Information	<input checked="" 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 checked="" type="checkbox"/> Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender)	<input checked="" 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 checked="" type="checkbox"/> Taxpayer Information/Tax Return Information	<input type="checkbox"/> Law Enforcement Information	<input checked="" type="checkbox"/> Security Clearance/Background Check Information
<input checked="" type="checkbox"/> Civil/Criminal History Information/Police Records (government source) (OF 306)	<input checked="" type="checkbox"/> Credit History Information (government source)	<input type="checkbox"/> Bank Secrecy Act Information
<input checked="" 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 (Auto-Assigned Applicant ID)	<input checked="" 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 checked="" 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	
<input type="checkbox"/> Other (please describe): _____	<input type="checkbox"/> Other (please describe): _____
<input type="checkbox"/> Other (please describe): _____	<input type="checkbox"/> Other (please describe): _____

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

Performance Assessment Network (PAN) Data feed	USAJOBS Data feed	Recruitment and Hiring Standard Forms
Specific PII identified in Section 4.2 that was acquired from this source: Information Listed Below	Specific PII identified in Section 4.2 that was acquired from this source: Information Listed Below	Specific PII identified in Section 4.2 that was acquired from this source: Standard Forms Listed Below
<i>Treasury Vacancy Request #</i> <i>Unique applicant id</i>	<i>Candidate ID</i> <i>Application ID</i> <i>Applicant Position Source</i> <i>Name: First, Middle, Last</i> <i>Legal Name Prefix, Suffix</i>	

<p><i>Unique secured URL</i></p> <p><i>Score</i></p>	<p><i>Home Address</i></p> <p><i>City/Town</i></p> <p><i>State/Territory/Province</i></p> <p><i>Country, Postal/Zip Code</i></p> <p><i>Telephone Number</i></p> <p><i>Applicant Email</i></p> <p><i>Veterans' Preference</i></p> <p><i>Country of Citizenship</i></p> <p><i>Race, Ethnicity, Sex</i></p> <p><i>Disability Indicator</i></p> <p><i>Veteran Indicator</i></p> <p><i>US Citizenship Indicator</i></p> <p><i>Selective Service</i></p> <p><i>Registration Indicator</i></p> <p><i>Federal Employment</i></p> <p><i>Status</i></p> <p><i>Current Employing Agency</i></p> <p><i>Current Fed-VRA</i></p> <p><i>Appointment Indicator</i></p> <p><i>Federal Retiree Indicator</i></p> <p><i>Buyout Indicator</i></p> <p><i>Employer Organization</i></p> <p><i>Name</i></p> <p><i>Contact Name</i></p> <p><i>Contact Phone</i></p> <p><i>Formal Title</i></p> <p><i>Employer Addresses</i></p> <p><i>Employer City/Town</i></p> <p><i>Employer State / Territory</i></p> <p><i>/ Province</i></p> <p><i>Employer Country</i></p> <p><i>Employer Postal / Zip</i></p> <p><i>Code</i></p> <p><i>Employment History</i></p> <p><i>Education Indicator</i></p> <p><i>School or Program Name</i></p> <p><i>School or Program City</i></p> <p><i>/Town</i></p> <p><i>School or Program</i></p> <p><i>State/Territory/Province</i></p> <p><i>School or Program</i></p> <p><i>Country</i></p> <p><i>Applicant Grade Point</i></p> <p><i>Average (GPA)</i></p> <p><i>Degree/Level Attained</i></p> <p><i>Degree / Program</i></p> <p><i>Academic Honors</i></p> <p><i>Licensures, and</i></p> <p><i>Certifications</i></p> <p><i>Military Service Start Date</i></p> <p><i>Military Service End Date</i></p> <p><i>Organization Name</i></p> <p><i>Organizational</i></p> <p><i>Affiliation/Role</i></p> <p><i>References Indicator</i></p> <p><i>Applicant Reference Type</i></p> <p><i>Applicant Reference Name</i></p> <p><i>Applicant Reference Title</i></p> <p><i>Applicant Reference Phone</i></p> <p><i>Applicant Reference Email</i></p> <p><i>Language Identifier</i></p> <p><i>Job Related Training</i></p> <p><i>Resume Additional</i></p> <p><i>Information</i></p> <p><i>Other Disability</i></p>	
--	---	--

Manner in which information is acquired from source by the Treasury project/system: (select all that apply):	Manner in which information is acquired from source by the Treasury project/system: (select all that apply):	Manner in which information is acquired from source by the Treasury project/system: (select all that apply):
<input checked="" type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input checked="" type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group
Please identify the form name (or description) and/or number (e.g., OMB Control Number): see below	Please identify the form name (or description) and/or number (e.g., OMB Control Number):	Please identify the form name (or description) and/or number (e.g., OMB Control Number):
<input checked="" type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.
<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.
<input checked="" type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input checked="" type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet
<input checked="" type="checkbox"/> Email	<input type="checkbox"/> Email	<input checked="" type="checkbox"/> Email
<input checked="" type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.	<input checked="" type="checkbox"/> Scanned documents uploaded to the system.
<input type="checkbox"/> Bulk transfer	<input checked="" type="checkbox"/> Bulk transfer	<input checked="" type="checkbox"/> Bulk transfer
<input checked="" type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
<input checked="" type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax
<input checked="" type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact
<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____

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 N/A 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.

All information provided in an application for a federal position is voluntary. In order to be considered for a position, however, all required application information must be submitted by the application deadline which is identified in the job posting. The applicant is responsible for ensuring that all application information provided is factually correct, in the format requested, and submitted by the job posting deadline. Required information not provided by the applicant may result in ineligibility. Agencies posting and hiring for a position follow all appropriate Federal regulations based on the type of job posting.

Use of Social Security Numbers

Social Security numbers (“SSNs”) are commonly used by identity thieves to commit fraudulent acts against individuals. The SSN is one data element that has a heightened ability to harm the individual and requires more protection when used. Therefore, in an effort to reduce risk to individuals and federal agencies, government-wide initiatives aimed at eliminating unnecessary collection, use, and display of SSN have been underway since OMB required agencies to review their SSN practices in 2007.

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 below explaining why other alternatives to identify individuals will not be used.*

Section 4.4(f) Yes No N/A Will an individual be denied any right, benefit, or privilege provided by law if the individual refuses 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 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 below how the notice is provided.*

Upon initial creation of an applicant profile, the full SSN is entered. The nine SSN digits are only displayed for a few seconds after entry and then changed to an asterisk. The full SSN is then truncated in future views of the applicant profile unless the applicant needs to change the number. View of an applicant's SSN (as part of the application) is managed by user permissions. Only users with access to application data (typically HR Specialists or Administrators) have privileges to view the last four digits of the SSN.

When the SSN is collected, individuals are notified whether disclosure is mandatory or voluntary, the legal authority by which the SSN is solicited, and what uses will be made of it.

Applicants get this popup message online or printed on a paper form: "Information regarding disclosure of your Social Security Number under Public Law 93-579 Section 7(b)(Privacy Act of 1974): Disclosure by you of your Social Security Number (SSN) is mandatory to obtain the services, benefits, or processes that you are seeking. Solicitation of the SSN by the Federal Agency is authorized under provisions of Executive Order 9397 dated November 22, 1943. The SSN is used as an identifier throughout your Federal career from the time of application through retirement. It will be used primarily to identify your records that you file with your Federal Agency. The SSN also will be used by the requesting Federal employer and other Federal Agencies in connection with lawful requests for information about you from your former employers, education institutions, and financial or other organizations. The information gathered through the use of the number will be used only as necessary in personnel administration processes carried out in accordance with established regulations and published notices of systems of records. The use of the SSN is made necessary because of the large number of present and former federal employees. Applicants who have identical names and birth dates can only be distinguished by SSN.

Providing false information, creating fake IDs, or failing to answer all questions truthfully and completely may be grounds for not hiring, for disbarment from federal employment, or for dismissal after the applicant begins work. Falsifying a federal job application, attempting to violate the privacy of others, or attempting to compromise the operation of this system may be punishable by fine or imprisonment (US Code, Title 18, section 1001)."

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\(i\)](#) 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.

Not applicable

[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.

Treasury and its CareerConnector customers in other federal agencies use the information collected and maintained in CareerConnector to effectively recruit, assess, certify, and onboard candidates for federal positions. The purpose of CareerConnector is to allow referral of interested and qualified applicants to hiring managers for vacancies to which they have applied and provide subscribing customers the ability to acquire, assess, certify, select, and onboard qualified candidates precisely, efficiently and cost-effectively. It provides the up-to-date tools agencies need for strengthening the employment foundation of government. All applicants' information provided to CareerConnector is needed to make the necessary suitability, eligibility, and qualification determinations and perform referrals. SSNs are collected in CareerConnector as an applicant identifier. The onboarding function in CareerConnector provides agency users with the ability to facilitate the electronic submission of onboarding form data entered by the new hire. The information applicants provide to Treasury and its CareerConnector customers is required to complete the pre-employment process and generate the personnel and payroll records for the new hire.

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?

Information provided by the applicant is initially used to make decisions regarding which applicants to interview. Non-IRS Treasury applicants who are elected for hire and accept a position at Treasury then submit their onboarding information via EODs, a different system covered by its own PCLIA. Applicants who accept IRS offers of employment submit the information necessary to process background clearances via CareerConnector. CareerConnector also services non-Treasury customers who maintain access privileges for their own agency/organization. Bureau of the Fiscal Service, a Treasury customer, has access to the data for customer agencies they service. CareerConnector does not actually send data to third parties but the data is made available to non-Treasury CareerConnector customers.

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](#)?
None of the information provided is used for data mining.

[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](#)?
CareerConnector maintains a system of records and none of the records are exempt from the Section (e)(5) accuracy, relevance, timeliness, and completeness requirements .

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.

[Section 5.2\(b\)](#) Yes No Is any of the information maintained in the system or by the project (a) part of a [system of records](#) and (b) used as part of a matching program?

[Section 5.2\(c\)](#) Yes No N/A Is there a matching agreement in place that contains the information required by Section (o) of the [Privacy Act](#)?

[Section 5.2\(d\)](#) Yes No N/A Are assessments made regarding the accuracy of the records that will be used in the matching program?

Section 5.2(e) Yes No 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 [Privacy Act](#) before taking adverse action against the individual?

There are no matching agreements in place between CareerConnector and any other system of record.

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.

Section 5.2(f) Yes 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?

Applying for a Federal job opening is voluntary and all information provided to complete an application is provided by the applicant. In order to be considered for a position, all required application information must be submitted by the application deadline which is identified in the job posting. The applicant is responsible for ensuring that all application information provided is factually correct, in the format requested, and submitted by the job posting deadline. The collected data is verified for accuracy, relevancy, and completeness by the applicants who submit their information to Treasury and other Federal agencies that use CareerConnector. Required information not provided by the applicant may result in ineligibility. Agencies posting and hiring for a position follow all appropriate Federal regulations based on the type of job posting. Information coming from USAJOBS related to the vacancy questions are confirmed by the applicant as accurate before it is sent to CareerConnector.

Merging Information About Individuals

Section 5.2(g) Yes 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)?

Section 5.2(h) Yes No N/A Once merged, is the information used in making determinations about 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?

CareerConnector receives applicant profile information, resume and supporting documentation from USAJOBS (electronic external source) which is associated with the applicant as they complete the application process in CareerConnector. The applicant information that Treasury and other CareerConnector customers receive from USAJOBS is used by human resources professionals to determine eligibility and qualifications and by hiring managers to make hiring decisions. CareerConnector customers who utilize third party assessment systems may have assessment scores transferred from the assessment vendor to CareerConnector.

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](#))?

Information coming from USAJOBS related to the vacancy questions is confirmed by the applicant for accuracy before it is sent to CareerConnector. The CareerConnector Program team works with vendor to ensure all system functionality works as expected to support recruitment processes, data collection and reporting, as well as continuity of data feeds between all systems (to ensure that the information remains up-to-date by allowing the applicant or employee to update their information). Any accuracy and completeness issues that are found within the system are escalated to the vendor and communicated and resolved according to the established Service Level Agreements. The information requested and collected in the forms listed above is narrowly tailored to what is relevant and required to accomplish CareerConnector functions. After Treasury review and scrutiny of all forms, the Office of Management and Budget reviews, scrutinizes and eventually approves all Treasury forms that are subject to the Paperwork Reduction Act. All reviews include ensuring that all information requested is relevant.

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?

During the development and interconnection process, data assurances are obtained from other federal IT systems' organizations that their data is correct – e.g., from USAJOBS, HRConnect, and Performance Assessment Network (PAN).

Applying for a Federal job opening is voluntary and all information provided to complete an application is provided by the applicant. In order to be considered for a position, all required application information must be submitted by the application deadline which is identified in the job posting. The applicant is responsible for ensuring that all application information provided is factually correct, in the format requested, and submitted by the job posting deadline. The data is verified for accuracy, relevancy, and completeness by the applicants who submit their information to Treasury and other Federal agencies that use CareerConnector. Required information not provided by the applicant may result in ineligibility. Agencies posting and hiring for a position follow all appropriate Federal regulations based on the type of job posting. Information coming from USAJOBS related to the vacancy questions are confirmed by the applicant as accurate before it is sent to CareerConnector.

The CareerConnector Program Team works with vendor to ensure all system functionality works as expected to support recruitment processes, data collection and reporting, as well as continuity of data feeds between all systems. Any issues that are found within the system are escalated to the vendor and communicated and resolved according to the established Service Level Agreements.

All information moved between systems through a data feed is managed according to the Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU) and the Functional Design Document that describe the data being moved, that format of the data, as well as the update intervals. Errors in the feeds must be corrected in the source system.

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?

The applicant is responsible for ensuring that their data input into USAJobs is accurate. PII corrections are completed in the source system by the applicant. If necessary, a human resources representative for the agency announcing the vacancy can assist the applicant in making changes.

[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 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”)?

Applicant information is restricted to Recruiting and Hiring Staff, and selection panels for that vacancy. Additionally, security roles are constrained to show only the information relevant to the staffing and recruiting work being conducted, generally at the bureau level. Disclosure of the information is made only after validating an appropriate routine use published in the SORN, identifying another relevant Privacy Act exception, or obtaining the consent of the individual.

Memorandum of Understanding (MOU)/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**?

MOU are in place for the following:

- CareerConnector to HRConnect Interconnection Security Agreement (ISA) Memorandum of Agreement (MoA)
- USAJOBS to CareerConnector Addendum for Master Interconnection Security Agreement (MISA); Treasury EBS CareerConnector to OPM-USAJOBS
- CareerConnector to PAN (Interconnection Security Agreement between EBS Career Connector and PAN)

Internal Information Sharing Chart

Internal Recipient’s Name (e.g., bureau or office)	HRConnect	Enterprise Data Management
Purpose of the Sharing	Data Feed Between Systems	Data Feed Between Systems
PII Shared	See Section 4.2 above.	See Section 4.2 above.
Applicable Statutory or Regulatory or Restrictions on Information Shared	<i>Disclosure of the information is made only after validating an appropriate routine use published in the SORN, identifying another relevant Privacy Act exception, or obtaining the consent of the individual.</i>	<i>Disclosure of the information is made only after validating an appropriate routine use published in the SORN, identifying another relevant Privacy Act exception, or obtaining the consent of the individual.</i>
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	NA	NA
Name and Description of MOU or Other Agreement Restricting Treasury’s Internal Use, Maintenance, Handling, or Sharing of PII Received	NA	NA
Method of PII Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/other (please describe if other)	Bulk Transfer	Bulk Transfer

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

External Information Sharing

Section 5.4(a) Yes No N/A Is [PII](#) maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?

External disclosure of the information is made only after validating an appropriate routine use published in the SORN, identifying another relevant Privacy Act exception, or obtaining the consent of the individual.

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 Act](#) 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 [record](#) that has been disclosed to the person or agency if an accounting of the disclosure was made?

Automated transfers of data from CareerConnector to other systems and from other systems to CareerConnector are date-stamped/logged. Therefore, an electronic log is maintained of electronic disclosures from the system to systems outside Treasury.

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)?

External disclosure of the information is made only after validating an appropriate routine use published in the SORN, identifying another relevant Privacy Act exception, or obtaining the consent of the individual.

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 Enterprise Business Solutions (EBS) (which manages CareerConnector) has Inter Agency Agreements (IAA) with each customer which describe data elements the system provides. CareerConnector is included in the IAA the Treasury Shared Service Center has with Treasury and non-Treasury customers. External disclosure of the information is made only after validating an appropriate routine use published in the SORN, identifying another relevant Privacy Act exception, or obtaining the consent of the individual.

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](#)?

Disclosure of the information is made only after validating an appropriate routine use published in the SORN, identifying another relevant Privacy Act exception, or obtaining the consent of the individual.

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 EBS has IAA with customers limiting release of applicants' data.

External Information Sharing Chart

[Section 5.4\(k\)](#) Yes No Is information from the system or project shared externally?

Performance Assessment Network (PAN)

External Recipient's Name	<i>PAN</i>	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.	Though it is technically not external sharing, infrastructure (in CareerConnector) is made available 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. These CareerConnector customers input their own agency data into the system. The data of each customer is segregated/partitioned from the data input by other CareerConnector customers (including Treasury).
Purpose of the Sharing and PII Shared	To provide all assessment services related to the hiring. The unique identifier ties an applicant and their score to their application in order for a hiring decision to be made. Information shared: Treasury Vacancy Request # Unique applicant id Unique, tokenized URL Score	When necessary to accomplish an agency function.	When necessary to accomplish an agency function.
Content of Applicable Routine Use/Citation to the SORN	See Section 6.1(b) below.	See Section 6.1(b) below.	See Section 6.1(b) below.
Applicable Statutory or Regulatory or Restrictions on Information Shared	The Privacy Act of 1974.	The Privacy Act of 1974.	The Privacy Act of 1974.

CareerConnector sends a unique identifier to PAN; the unique identifier is not tied to the applicant's User Id

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

Section 5.4(i) 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))?

When applicants sign in to CareerConnector via USAJOBS, they are provided with and consent to the online Full Terms and Conditions of Use. These terms and conditions inform the applicants that their access and use of USAJOBS and CareerConnector constitutes their consent for Treasury and CareerConnector customers to review all information on the system and disclose information as necessary to monitor, record, audit, and take action as necessary to process their applications. Users are also notified that their information may be disclosed to authorized government and law enforcement personnel as allowed by law. For vacancies that require online assessments, the applicant is informed that information will be shared with CareerConnector. Applicants who do not want to consent to the outlined uses may choose not to apply. There are no disclosures of previously collected records in the system of records not expressly authorized by the Privacy Act or contained in the routines uses in the published SORNs.

[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](#)?

Treasury .001 - Treasury Payroll and Personnel System - 81 FR 78266 (Nov. 7, 2016)

DO .191 - Human Resources and Administrative Records System - 81 FR 78298

IRS 90.006 - Chief Counsel Human Resources and Administrative Records - 80 FR 54063

BPD .001 - Human Resources and Administrative Records - 76 FR 51128 (Aug. 17, 2011)

FMS .005 - FMS Personnel Records - 77 FR 62602 (Oct. 15, 2012)

IRS 36.003 - General Personnel and Payroll Records - 80 FR 54063 (Sept. 8, 2015)

OPM/GOVT-1 - General Personnel Records December 11, 2012 77 FR 73694

OPM/GOVT-5 Recruiting, Examining and Placement Records

OPM/GOVT-6 - Personnel Research and Test Validation Records June 19, 2006 71 FR 35354

[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?

The CareerConnector system collects information from applicants who are members of the public, applicants who may be current or former federal employees or former members of the armed forces.

[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?

System covered under GRS 2.1, items 050 and 060

[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?

The CareerConnector System underwent the latest SA&A in June 2019. The CareerConnector System has an active ATO dated January 2018 and expires January 2021.

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?

The use of access controls restricts the ability to retrieve data based on an individual's authorization and access permissions that are built into the system. The system maintains access roles that restrict and grant access to information and functionality to support the unique business process needs of a subscribing agency. Access is provided through access controls built into CareerConnector, only to authorized and registered agency users. When agency users are authorized to access CareerConnector, they are informed regarding the appropriate use of the information it contains and agree to adhere to the Rules of Behavior. Access is controlled and limited based on unique user identification and authentication mechanisms. Access to the CareerConnector requires unique user identification and corresponding password. Roles are assigned to unique user identifiers

Privileged functions including system control, monitoring, or administration are only performed by authorized personnel (i.e., personnel determined by assigned official duties and satisfying all personnel security criteria). All root and privileged functions can only be accessed from a valid account and will be audited.

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)?

No risks were identified in the manner in which the data is collected.

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?

Treasury security requirements are met in the method of transferring information.

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?

With the approval and implementation of the latest CareerConnector Access Control Policy, user accounts and activities are reviewed monthly to ensure that the activities are appropriate and within the authorized boundaries. Any anomalies are reported and investigated.

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?

Per CareerConnector System Security Plan (SSP) Control; "AU-6 (1) (3) Audit Review, Analysis, And Reporting" the CareerConnector application and its databases are monitored using the tool IP Monitor. Additionally, the database is monitored using grid control.

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)?

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?

Monster Government Solution's compliance with Section 508 was evaluated using Interagency Trusted Tester Program (ITTP)/Department of Homeland Security (DHS) Office of Accessible Systems & Technology (OAST) Trusted Web Accessibility Tool (WAT) and Job Access With Speech (JAWS). New Editions Consulting conducted the independent evaluation. The evaluation covered Levels A, AA, and AAA accessibility frameworks.

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 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](#)?

This records in the relevant Systems of Records are not exempt from 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)?

Once an applicant have creates a user name and password and signs in through USAJOBS, they can access their information in Career Connector. In addition, each SORN identified in Section 6.1(b) provides individuals with information concerning how to request particular types of records that Treasury may have about them.

Approval Signature

Timothy H. Skinner
Bureau Privacy and Civil Liberties Officer
Departmental Office, & Records