Privacy and Civil Liberties Impact Assessment
for

# inCompass

April 2, 2018


**Reviewing Official**
Ryan Law
Deputy Assistant Secretary for Privacy, Transparency, and Records
Department of the Treasury

**Bureau Certifying Official**
Timothy H. Skinner
Bureau Privacy and Civil Liberties Officer
Office of Privacy, Transparency, and Records
Department of the Treasury

## Section 1: Introduction

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

This assessment is being completed pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget ("OMB") Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before:

1. developing or procuring information technology ("IT") systems or projects that collect, maintain or disseminate PII from or about members of the public, or

2. initiating a new collection of information that: a) will be collected, maintained, or disseminated using IT; and b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons. Agencies, instrumentalities, or employees of the federal government are not included.

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

*This PCLIA supersedes the Privacy Impact Assessment for this system dated August 3, 2011.*

## Section 2: Definitions

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

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

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

**Contractors and service providers** – are private companies that provide goods or services under a contract with the Department of the Treasury or one of its bureaus. This includes, but is not limited to, information providers,

information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

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

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

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

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

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

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

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

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

**Information** – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. This term includes, but is not 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 PCLIAs 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

*Treasury maintains a blanket purchase agreement (BPA) with a company named CornerstoneOnDemand (CSOD) which provides a unified talent management software application. CSOD owns the software, hosts this software on its own servers, and makes it available to customers through a licensing subscription model via the internet (a distribution model known as "Software-as-a-Service"). CSOD is a commercial off-the-shelf (i.e., ready to use) product that Treasury and other agencies use to support their Human Resource (HR) functions. CSOD is a comprehensive talent management system that supports automation and cross-program collaboration for HR programs. It covers the processing of HR data (for the purposes described below) for participating agencies from the time an employee is hired by the agency through retirement. This product suite incorporates the following functional modules that are closely aligned with both established and emerging federal agency HR programs:*

| ***CSOD Modules*** | | |
|---|---|---|
| | ***Module Name*** | ***Module Functional Description*** |
| ***1*** | *Compensation Management ("CSOD Award")* | *CSODAward streamlines award programs to better motivate employees to focus on achieving strategic objectives and mission. It promotes accountability, productivity, and retention by simplifying compensation planning, incentive management, budgeting, and reporting. CSOD Award easily accommodates hourly, salaried, or commissioned employees, and short- and long-range compensation plans.*<br>*Key Features & Functions: Integrated Salary and Performance Data, Compensation Programs, Incentive Management, Pay-for-Performance, Budgeting & Reporting* |
| ***2*** | *Connect – Asynchronous Learning (CSOD Connect")* | *CSOD Connect provides collaboration tools for formal and informal learning, feedback, coaching, mentoring, and communities of interest. It is a powerful collaboration tool for engaging employees, and enables agencies to readily access information and resources. CSOD Connect blends seamlessly with recruiting, learning, and performance review activities.* |

| ***CSOD Modules*** | | |
|---|---|---|
| | ***Module Name*** | ***Module Functional Description*** |
| | | *Key Features & Functions: Employee Bio & Profile, Social Feedback, Real-time Activity Updates, Team Tasks Management* |
| ***3*** | *EDGE ("CSOD Edge")* | *CSOD Edge simplifies integration with other workforce applications to optimize agencies' human capital technology investment. It is a flexible way to extend the inCompass solution to other applications without the complexity and cost of building and maintaining custom integrations.*<br>*Key Features & Functions: Marketplace, Integration Management* |
| ***4*** | *Employee Planning ("CSOD Planning")* | *CSOD Planning transforms workforce data into a vacancy management plan to support agency right-sizing and drive effective human capital decisions. It is a purpose-built tool which provides intuitive, interactive, and visual workforce planning to make sure agencies have the right talent in the right roles at the right time.*<br>*Key Features & Functions: Headcount Planning, Co-Planning, Customized Costing Models* |
| ***5*** | *Employee View ("CSOD View")* | *CSOD View employs interactive visualization tools to gain insights on workforce data and inform smart human capital decisions at any time. It enables leadership to visually explore talent data to draw talent conclusions, and make the right talent decisions.*<br>*Key Features & Functions: Diagnostic Analytics, List Creation, Filters* |
| ***6*** | *Extended Enterprise ("CSOD Extended Enterprise")* | *CSOD Extended Enterprise supports delivery of training outside of the organization. Training provided may be for a fee. The type of information collected for this module includes individual data for identifying the person for training records management and related information for commercial transactions.* |
| ***7*** | *Insights / Analytics ("CSOD Analytics")* | *CSOD Analytics creates self-service real-time reports to solve critical workforce issues, and better recruit, manage, develop, reward, and retain employees. It enables leaders to answer burning workforce questions, and take immediate action within the inCompass solution to address issues or risks.*<br>*Key Features & Functions: Compliance Guide, Compliance Control, Learning Optimization, Predictive Succession* |
| ***8*** | *Learning Management ("CSOD Learning")* | *CSOD Learning empowers individuals with personalized training programs and certification paths which develop their specific competencies and skills needs. It serves as a single point of access to deliver robust e-Learning experiences, mobile learning, and administer instructor-led training (ILT) and virtual classroom sessions. CSOD Learning enhances employee performance, supports compliance, and fosters collaboration within your organization.*<br>*Key Features & Functions: Offline Player, Course Publisher, Mobile Learning, Video Streaming, Groups & Communities, Document Management, Automated Registration & Roster Administration* |
| ***9*** | *LINK ("CSOD Link")* | *CSOD Link improves data accuracy and process completion time through self-service forms, and standardizes approval processes. It quickly and cost effectively centralizes employee data to give human resources teams more meaningful reporting to inform strategic talent strategies. CSOD Link engages employees through self-service, and streamlines administrative processes.*<br>*Key Features & Functions: Customized Forms, Dynamic Fields, Automated Document Routing & Tracking, Data Visualization.* |
| ***10*** | *Onboarding – Employee Acculturation ("CSOD Onboarding")* | *CSOD Onboarding links new hires to learning resources, job-related tools, and organizational connections – empowering them to become integrated into the organization and productive faster. It delivers the right resources, connections, and tools which quickly familiarize new hires with organization culture, work colleagues, learning resources, and performance goals. CSOD Onboarding- does NOT support benefits enrollment or other core HR employee onboarding tasks (which are* |

| *CSOD Modules* | | |
|---|---|---|
| | ***Module Name*** | ***Module Functional Description*** |
| | | *performed by HRConnect or other Shared Service Providers).*<br>*Key Features & Functions: Personalized & Branded Welcome Pages, Onboarding Tasks & Check Lists, Centralized New Hire Portal, Onboarding Dashboards* |
| ***11*** | *Performance Management ("CSOD Performance")* | *CSOD Performance aligns individual, departmental, and agency goals to translate workforce activities into positive business results. It delivers goal management, competency tracking, and career management functionality to optimize organizational operations and effectively reward talent.*<br>*Key Features & Functions: Goal/Element Setting, Custom Performance Reviews, 360-Degree Reviews, Configurable Competency Models, Managerial Comments & Feedback, Career Development Plans* |
| ***12*** | *Recruiting ("CSOD Recruiting")* | *CSOD Recruiting employs industry-leading talent acquisition tools to help you find the right people for your agency's workforce needs, and tracks hiring-related metrics. It enables agencies to reach targeted talent directly with matching technology for social network profiles, and building in tools to encourage, manage, and measure recruitment progress.*<br>*Key Features & Functions: Application Management, Configurable Workflows, Requisition Management, Employee Referral Engine, Social Network Integration, Candidate Profiles* |
| ***13*** | *Succession Management ("CSOD Succession")* | *CSOD Succession applies organizational metrics and results to build and cultivate candidates for at-risk, mission-critical, and executive positions. It streamlines every aspect of workforce succession planning. Succession serves both the employee and executive team with easy to build organizational models and develop.*<br>*Key Features & Functions: 9-Box Grid, Succession Scenarios, Internal Candidate Search.* |

*Treasury Enterprise Business Solutions (EBS) offers CSOD to other federal agencies via Treasury's BPA. As of 2018, the following federal agencies are using CSOD:*

- *Consumer Financial Protection Bureau (CFPB);*
- *Department of Housing and Urban Development (HUD);*
- *HUD Office of the Inspector General (OIG);*
- *Small Business Administration (SBA);*
- *Department of the Treasury (rolling off September 30, 2018); and*
- *United States Agency for International Development (USAID).*

*With the exception of SBA, all of the CSOD users are also shared services users of Treasury's HRConnect System. HRConnect collects all Treasury (and other participating agency) employee data from the date of hire through retirement (as stated above, inCompass merely processes certain HRConnect data for specific purposes from hiring to retirement). Please refer to the HR Connect PCLIA which can be found on the Treasury Privacy Page at https://www.treasury.gov/privacy/issuances/Pages/default.aspx. The CSOD system is populated with limited data fed to the participating agency (except SBA) from its HRConnect portal. The particular data elements received from HR Connect are discussed in section 4.2 of this PCLIA. The data elements inCompass receives from HRConnect are the same for all participating agencies. CSOD supports agency HR functions by providing an environment where the data can be securely processed to perform the day-to-day operations discussed in the description of the modules above.*

*Each agency that uses CSOD has their own portal and owns their own data. Data is not shared across participating agency portals. Each portal has three different system environments: Production, Stage, and Pilot. Production is*

*the agencies' live environment where all agency users perform tasks. Stage environment is used by privileged access users to test how new software releases interact with current system configurations. This allows the agency to assess organizational and security impact (including security testing) of a new software release before it goes live (i.e., into production). Pilot environment is where privileged access users test proposed changes to system configurations and workflow and experiment with available functionality that has not yet been deployed in the Production environment.*

*Although the commercial name for the product is CSOD, the agencies that use the system have renamed (or rebranded) their specific agency portals to meet their own needs.*

- *Treasury, HUD and CFPB – inCompass;*
- *SBA – Talent Management Center;*
- *USAID – USAID University;*

*For the remainder of this PCLIA, the system will be referred to as "CSOD" or "the system"; the governing program office will be referred to as "inCompass Program Office"; and end-users will be referred to as "agency".*

*The other federal agencies that use the system have the option of relying on this PCLIA or conducting their own Privacy Impact Assessment.*

### Section 3.2: Authority to Collect

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

- *5 U.S.C. § 301, Departmental regulations - Department regulations for the operations of the Department, conduct of employees, distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.*
- *31 U.S.C. § 321, General authority of the Secretary - General authorities of the Secretary establish the mission of the Department of the Treasury.*
- *Homeland Security Presidential Directive 12 (HSPD-12) – requires the development and agency implementation of a government-wide standard for secure and reliable forms of identification for federal employees and contractors.*
- *e-Government Act of 2002 (H.R. 2458/S. 803) supports cross- services initiatives to reduce federal government expenditures.*

## 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
5. ☐ 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?

*The records in this system are covered by the Office of Personnel Management (OPM)/GOVT-1, General Personnel Records, system of records notice (SORN) (December 11, 2012, 77 FR 73694). None of the records in this government-wide SORN are exempt from the relevant and necessary requirement under the Privacy Act.*

*Most of the data maintained in inCompass is derived from Treasury's HRConnect system. The purpose of the HR Connect system is to support the human resources functions for the Department of the Treasury and other federal agencies that use HR Connect, or another shared service provider, as part of a cross- services initiative to reduce federal government expenditures. The inCompass program also continuously reevaluates its PII to ensure that the data it collects is limited to PII that is relevant and necessary to perform functions in CSOD. After HRConnect data is transferred to CSOD, the inCompass program team performs an annual review process to evaluate the data feed to ensure that the information populating the system is still relevant and necessary for CSOD to work as designed. The inCompass program team looks at the current data feed and compares the data collected against the new functionality deployed or newly available to determine potential efficiencies that could be gained through additional data elements or structurally changed data. If there are opportunities to make improvements, the inCompass program team works with the HRConnect team to institute these changes.*

## 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.

| Biographical/General Information | | |
|---|---|---|
| ☒ Name | ☐ Gender | ☐ Group/Organization Membership |
| ☐ Date of Birth | ☐ Race | ☐ Military Service Information |
| ☐ Home Physical/Postal Mailing Address | ☐ Ethnicity | ☐ Personal Home Phone or Fax Number |
| ☐ Zip Code | ☐ Personal Cell Number | ☐ Alias (including nickname) |
| ☒ Business Physical/Postal Mailing Address | ☐ Business Cell Number | ☐ Business Phone or Fax Number |
| ☐ Personal e-mail address | ☐ Nationality | ☐ Mother's Maiden Name |
| ☒ Business e-mail address | ☐ Country of Birth | ☐ Spouse Information |
| ☐ Personal Financial Information (including loan information) | ☐ City or County of Birth | ☐ Children Information |
| ☐ Business Financial Information (including loan information) | ☐ Immigration Status | ☐ Information about other relatives. |
| ☐ Marital Status | ☐ Citizenship | ☐ Professional/personal references or other information about an individual's friends, associates or acquaintances. |
| ☐ Religion/Religious Preference | ☐ Device settings or preferences (e.g., security level, sharing options, ringtones). | ☒ Global Positioning System (GPS)/Location Data<br>**Geolocation – see Section 4.3* |
| ☐ Sexual Orientation | ☒ User names, avatars etc.<br>**HRConnect User Name / HRConnect User ID / Manager ID* | ☐ Secure Digital (SD) Card or Other Data stored on a card or other technology |
| ☐ Cell tower records (e.g., logs. user location, time etc.) | ☐ Network communications data | ☐ Cubical or office number |
| ☐ Contact lists and directories (known to contain personal information) | ☐ Contact lists and directories (not known to contain personal information, but uncertain) | ☐ Contact lists and directories (known to contain only business information) |
| ☒ Education Information | ☐ Resume or curriculum vitae | ☐ Other (please describe): |

| Identifying Numbers | |
|---|---|
| ☐ Full Social Security number | ☐ Health Plan Beneficiary Number |
| ☐ Truncated/Partial Social Security number (e.g., last 4 digits) | ☐ Alien Registration Number |
| ☐ Personal Taxpayer Identification Number | ☐ Business Taxpayer Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor) |
| ☐ Personal Credit Card Number | ☐ Business Credit Card Number (If known: ☐ sole proprietor; ☐ non-sole proprietor) |
| ☐ Personal Vehicle Identification Number | ☐ Business Vehicle Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor) |
| ☐ Personal License Plate Number | ☐ Business License Plate Number (If known: ☐ sole proprietor; ☐ non-sole proprietor) |
| ☐ File/Case ID Number (individual) | ☐ File/Case ID Number (business) (If known: ☐ sole proprietor; ☐ non-sole proprietor) |
| ☐ Personal Professional License Number | ☐ Business Professional License Number (If known: ☐ sole proprietor; ☐ non-sole proprietor) |

| | |
|---|---|
| ☒ Employee Identification Number<br>**HR Connect Employee ID* | ☐ Patient ID Number |
| ☐ Business Bank Account Number | ☐ Personal Bank Account Number |
| ☐ Commercially obtained internet navigation/purchasing habits of individuals | ☐ Government obtained internet navigation/purchasing habits of individuals |
| ☐ Business License Plate Number (non-sole-proprietor) | ☐ Driver's License Number |
| ☐ Personal device identifiers or serial numbers | ☐ Other Identifying Numbers (please describe):_____ |
| ☐ Passport Number and Passport information (including full name, passport number, DOB, POB, sex, nationality, issuing country photograph and signature) (use "Other" if some but not all elements are collected) | |

| Medical/Emergency Information Regarding Individuals | | |
|---|---|---|
| ☐ Medical/Health Information | ☐ Worker's Compensation Act Information | ☐ Patient ID Number |
| ☐ Mental Health Information | ☐ Disability Information | ☐ Emergency Contact Information (e.g., a third party to contact in case of emergency) |
| ☐ Other (please describe): _____ | | |

| Biometrics/Distinguishing Features/Characteristics of Individuals | | |
|---|---|---|
| ☐ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.) | ☐ Signatures | ☐ Vascular scans |
| ☐ Fingerprints | ☐ Photos | ☐ Retina/Iris Scans |
| ☐ Palm prints | ☐ Video | ☐ Dental Profile |
| ☐ Voice audio recording | ☐ Scars, marks, tattoos | ☐ DNA Sample or Profile |
| ☐ Other (please describe): _____ | ☐ Other (please describe): _____ | ☐ Other (please describe): _____ |

| Specific Information/File Types | | |
|---|---|---|
| ☐ Taxpayer Information/Tax Return Information | ☐ Law Enforcement Information | ☐ Security Clearance/Background Check Information |
| ☐ Civil/Criminal History Information/Police Records (government source) | ☐ Credit History Information (government source) | ☐ Bank Secrecy Act Information |
| ☐ Civil/Criminal History Information/Police Records (commercial source) | ☐ Credit History Information (commercial source) | ☐ National Security/Classified Information |
| ☐ Protected Information (as defined in Treasury Directive 25-10) | ☐ Case files | ☒ Personnel Files<br>**Performance records, training records, award record, competency assessments, etc.* |
| ☐ Information provided under a confidentiality agreement | ☐ Information subject to the terms of an international or other agreement | ☒ Other (please describe): Employment history |

| Audit Log and Security Monitoring Information | | |
|---|---|---|
| ☐ User ID assigned to or generated by a user of Treasury IT | ☒ Date and time an individual accesses a facility, system, or other IT | ☐ Files accessed by a user of Treasury IT (e.g., web navigation habits) |
| ☒ Passwords generated by or assigned to a user of Treasury IT | ☐ Internet or other queries run by a user of Treasury IT | ☐ Contents of files accessed by a user of Treasury IT |
| ☐ Biometric information used to access Treasury facilities or IT | ☐ Video of individuals derived from security cameras | ☐ Public Key Information (PKI). |
| ☐ 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 | ☐ Still photos of individuals derived from security cameras. | ☐ Internet Protocol (IP) Address |
| ☐ Other (please describe): | ☐ Other (please describe): | ☐ Other (please describe): _____ |

| Other |
|---|
| ☒ Other (please describe:<br><br>*Activities accomplished in CSOD can produce the following information associated with an employee:*<br>• *Training attendance / completion tracking*<br>• *Performance goals and assessment of progress toward those goals and year end ratings*<br>• *Individual goals aligned with organizational goals or strategies*<br>• *Competency assessment results*<br>• *Limited resume data provided voluntarily by the employee*<br>• *Annual award amounts*<br>• *Certification tracking and progress toward maintaining / acquiring certification*<br>• *Current and previous held positions*<br>• *Self-disclosed career interests* |

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

| HRConnect | Interior Business Center (IBC) | End User |
|---|---|---|
| **Specific PII identified in Section 4.2 that was acquired from this source:**<br><br>• HRConnect User ID<br>• HRConnect Employee ID<br>• First Name<br>• Middle Name<br>• Last Name<br>• Business Email | **Specific PII identified in Section 4.2 that was acquired from this source:**<br><br>• First Name<br>• Middle Name<br>• Last Name<br>• Business Email<br>• GeoLoc*<br>• Manager ID<br>• Business Address | **Specific PII identified in Section 4.2 that was acquired from this source:**<br><br>• Self-Disclosed Resume and Education Data<br>• Self-Disclosed Career Interests |

| | | |
|---|---|---|
| • GeoLoc*<br>• Manager ID<br>• Business Address | | |
| **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):** |
| ☐ From a paper or electronic form provided to individuals, the public or members of a particular group | ☐ From a paper or electronic form provided to individuals, the public or members of a particular group | ☐ 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): _____ | 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): _____ |
| ☐ Received in paper format other than a form. | ☐ Received in paper format other than a form. | ☐ Received in paper format other than a form. |
| ☐ Delivered to the project on disk or other portable device and uploaded to the system. | ☐ Delivered to the project on disk or other portable device and uploaded to the system. | ☐ Delivered to the project on disk or other portable device and uploaded to the system. |
| ☐ Accessed and downloaded or otherwise acquired via the internet | ☐ Accessed and downloaded or otherwise acquired via the internet | ☐ Accessed and downloaded or otherwise acquired via the internet |
| ☐ Email | ☐ Email | ☐ Email |
| ☐ Scanned documents uploaded to the system. | ☐ Scanned documents uploaded to the system. | ☐ Scanned documents uploaded to the system. |
| ☒ Bulk transfer (automated data feed from HRConnect nightly Mon.-Fri.) | ☒ Bulk transfer (manual as determined by agency) | ☐ Bulk transfer |
| ☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices). | ☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices). | ☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices). |
| ☐ Fax | ☐ Fax | ☐ Fax |
| ☐ Extracted from notes of a phone interview or face to face contact | ☐ Extracted from notes of a phone interview or face to face contact | ☐ Extracted from notes of a phone interview or face to face contact |
| ☒ Other: Please describe:<br>** A Geographic Location Code (GEOLOC) is an alphanumeric code that federal agencies use to identify geographic location. Use of these codes facilitates the interchange of data* | ☒ Other: Please describe:<br>** A Geographic Location Code (GEOLOC) is an alphanumeric code that federal agencies use to identify geographic location. Use of these codes facilitates the* | ☒ Other: Please describe:<br>*Employees are provided the option to enter, if they so choose, details specific to their professional and educational experience and career interests* |

| | | |
|---|---|---|
| *between federal agencies, state and local groups. The codes are in the format ABBCCCCDDD where A represents Country, BB is a two-digit State code, CCCC is a four-digit City code, and DDD is a three-digit County code. The state, city, and county codes are maintained by the Geographic Names Information System (GNIS), and the country codes from the GeoNet Names Server (GNS) registry maintained by the National Geospatial Intelligence Agency.* | *interchange of data between federal agencies, state and local groups. The codes are in the format ABBCCCCDDD where A represents Country, BB is a two-digit State code, CCCC is a four-digit City code, and DDD is a three-digit County code. The state, city, and county codes are maintained by the Geographic Names Information System (GNIS), and the country codes from the GeoNet Names Server (GNS) registry maintained by the National Geospatial Intelligence Agency.* | *to a resume/profile function within inCompass. These voluntary fields are populated by the employee.* |
| ☒ Other: Please describe:<br>*Current federal agencies providing data for use in the system:*<br>• *CFPB;*<br>• *HUD;*<br>• *HUD OIG;*<br>• *Treasury; and*<br>• *USAID.* | ☒ Other: Please describe:<br>*Small Business Administration* | ☐ 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 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.

*No privacy and civil liberties issues were identified in answering the questions in this section. PII is collected through the nightly (Monday-Friday) data feed from HRConnect (all participating agencies except SBA) and bulk data load from the I(SBA only). All of the PII in HR Connect that is fed to inCompass is collected directly from individual employees.*

*The only PII that is collected directly from employees within inCompass (as opposed to being collected for use in HRConnect and shared with inCompass) is certain resume and career goal information (including knowledge, skills, abilities, certifications, etc.). Employees provide this information on a voluntary basis. It is used to provide a baseline of internal talent within Treasury or one of its bureaus or offices to determine what skills need to be hired or developed to meet current and future organizational needs. Employees can view the skills required for certain positions and determine whether their skills are closely matched with those required for particular Treasury positions for which they may want to apply when positions become available. This also allows employees who do not currently have the necessary skills to use their career development plans to target acquisition of those skills allow them to work towards career progression. A Privacy Act Statement will be included at all points within the system where PII is collected from Treasury employees.*

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

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

☐ SSN disclosure is required by Federal statute or Executive Order. ; or

☐ the SSN is disclosed to any Federal, state, or local agency maintaining a system of records in existence

and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *If checked, please provide the name of the system of records in the space provided below.*

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

*inCompass does not collect or use SSNs. Therefore, no privacy and civil liberties risks were identified.*

## 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.

*Neither CSOD nor the inCompass program office collect or maintain any information describing how an individual exercises their rights guaranteed by the First Amendment. Therefore, no privacy or civil liberties risks were identified.*

# 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.

*CSOD is a comprehensive talent management system that supports automation and cross-program collaboration within each inCompass participating agency. Please see section 3.1 for a discussion about the CSOD modules and how data is used across the application.*

### 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)?<br><br>**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?<br><br>**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? |
| *CSOD is not designed to be used to make adverse determinations about individuals. CSOD does, however, contain performance evaluations and performance ratings that could be used as artifacts to support HR policies that could be used by an Agency's HR department to make an adverse determination about an individual's rights, benefits, and privileges under federal programs. The performance process is owned by HR and allows employees to input information into the system, as per policy, and any adverse actions would be made by the agency HR team and the guiding HR policy and processes for such matters. Each participating agency is responsible for corrections to its own data. Each agency follows its own processes for handling corrections to data and providing employees an opportunity to explain or correct the data before any adverse action is taken.* |

### 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? |
| *The information maintained in CSOD is not used to conduct data mining. Therefore, no privacy and civil liberties risks were identified.* |

## Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared

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

The Privacy Act requires that federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5). If a particular system of records meets certain

requirements (including the NPRM process defined in Section 2 above), an agency may exempt the system of records (or a portion of the records) from this requirement.

| |
|---|
| **Section 5.2(a)** ☐ Yes ☒ No Is all or any portion of the information maintained in the system or by the project: (a) part of a system of records and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the Privacy Act? |
| *None of the information maintained in the system is both part of a system of records and exempt from the accuracy, relevance, timeliness, and completeness requirements of the Privacy Act. None of the records in this system that are subject to the Privacy Act are exempt from any Privacy Act 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?<br><br>**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?<br><br>**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?<br><br>**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? |
| *Data contained in each agency's portal is not used as part of a computer matching program. Therefore, no privacy or civil liberties issues related to matching programs were identified.* |

## 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?

*Performance ratings and performance awards generated in CSODare transmitted or uploaded into the human capital management application in HRConnect. Ratings and awards are then sent to the National Finance Center (NFC), which maintains the official HR record. The NFC is responsible for reporting to the Office of Personnel Management's (OPM) Enterprise Human Resources Integration (EHRI) data warehouse and electronic Official Personnel Folder (eOPF).*

*Most performance ratings for an employee using the CSOD performance module are finalized in CSOD and, once approved by all required parties, are transmitted to HRConnect via mass upload excel spreadsheet. Ratings are then inserted in the Employee Review table. At the next execution of the nightly interface to NFC, ratings are transmitted to NFC. The ratings are reported to OPM on the regular reporting schedule. Note that ratings can be entered directly into HRConnect. This is typically an exception to standard operating procedure. The nightly transmission from CSOD runs Monday through Friday.*

*Performance awards are determined and approved in CSOD, and a spreadsheet is generated once approvals are final. The spreadsheet is then uploaded using the HRConnect mass update module. The awards are inserted as personnel actions in HRConnect and are transmitted to NFC at the next execution of the nightly NFC interface. The awards are reported to OPM on the regular reporting schedule. Note that awards (like ratings) can be entered directly into HRConnect, rather than having the information. This is typically an exception condition.* Either of the following would be an exception condition for award entry directly into HRConnect.

1. A rating change based on a successful grievance by an employee
2. A rating given later than the normal rating period end date to allow an employee to be on standards for 90 days

*The nightly transmission from CSOD runs Monday through Friday. Awards are not transmitted automatically via the nightly data feed to HRConnect from CSOD because of the frequency at which awards are changed after they are approved in CSOD, and the difficulty in reversing an award once it is paid.*

*Each participating agency is responsible for corrections to its own data. Each agency follows its own processes for handling corrections to data and providing employees an opportunity to explain or correct the data before any adverse action is taken.*

## 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?

*Neither CSOD nor the inCompass program office merge data with another system. CSOD sends performance ratings and performance awards to HRConnect, and HRConnect sends the ratings and awards information to NFC. CSOD sends training data to the HRConnect border server, where HRConnect associates that information to the SSN and date of birth of the employee record, before it transmits the file to OPM. Matching the SSN in HRConnect with the employee ID in inCompass files ensures that the correct information is aligned with the correct employee before it is sent to OPM.*

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

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

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

*The only automated feature in the process that ensures the accuracy, completeness, and timeliness of the information is the nightly feeds from HRConnect that freshen the data in CSOD for the next day. This ensures that any changes made to an employee's PII in HRConnect will be available the following day in CSOD. As stated above, the PII in CSOD is not designed for making adverse determinations about individuals, but the data may be used as an artifact in making an adverse decision. The nightly feeds ensure that those potential artifacts currently reflect the employee's file content in HRConnect.*

## 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?

*Data is collected and imported into inCompass from HR systems containing a complete set of employee HR data, like HRConnect (or another system within an inCompass participating agency). HR data imported into the system from an HR system is validated during the import process. Agency end-users and system administrators may review and provide feedback on the accuracy of the data in the system. It is the agency's responsibility to correct any errors found. Additionally, for every night the automated feed runs or a manual update is uploaded, the system produces and emails an "error log" so that specific errors can be identified and corrected by the agency owning the data.*

*The data imported into CSOD is as current as the information contained in the systems that are feeding data to CSOD. Data manually uploaded into CSOD is as current as the records being used to create the file to be uploaded. Information that is out of date needs to first be corrected in the originating system. Once the originating system is corrected, the information in inCompass will update through overnight processing, or manual upload, based on agency preference.*

*The agency using CSOD is ultimately responsible for the state of their data. Users may review and provide feedback on the accuracy of the data in the system. With an automated data feed, if there are errors, an error report is*

*generated each night the feed runs, specifically identifying errors that prevent the system from updating core user information. When a manual feed is run, if there are errors, the error reports generate upon completion of the upload. The error report identities the issue and allows for correction of the data from the source system before the next feed occurs.*

### 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 agency using CSOD is ultimately responsible for the state of their data. PII collected by CSOD is, with one exception, received by HRConnect. The exception is SBA, which receives its data feed from the Interior Business Center (IBC). The data feeds and their content are the responsibility HR and IBC. These processes for these systems ensure the data provided is corrected when needed. Once the originating system is corrected, the information in inCompass is automatically updated nightly, or by manual upload, depending on agency preference. Because the HRConnect data feed runs nightly, any correction made to HRConnect will be reflected in CSOD the following business day. With an automated data feed, if there are errors, an error report is generated each night the feed runs, specifically identifying errors that prevent the system from updating core user information. When a manual feed is run, like the data SBA uploads from IBC, if there are errors, the error reports generate upon completion of the upload. The error report identifies the issue and allows for correction of the data from the source system before the next feed occurs.*

*Additionally, with specific and limited exceptions, end users can enter education information, career interests and resume details within inCompass. It is the individual's responsibility to maintain and correct these details, as the data is not collected and received any other way. Users may review and provide feedback on the accuracy of the data in the feeder system (HR Connect or IBC) system at any time.*

*Additionally, each agency's HR program office is responsible for testing the configured business process and workflow to ensure accurate and desired results are achieved. If there is an error, it is the responsibility of the participating agency to take appropriate steps to correct the data.*

## 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")?

*Data is collected and imported into inCompass from HR systems containing core employee data, like HRConnect or another shared service provider's system.*

*The following classes of users will have some type of rights to access data in CSOD through reports, or the employee profile information, determined by system enforced defined permissions and constraints. Privileged account audits are conducted regularly as part of the standard governance model. And each agency's portal*

*supports restricting views based upon the agency's business need and segment of the population:*

- *The employee has access to their own information.*
- *The employee's supervisor and superiors within their chain of command because they need to know the information to perform their supervisory duties.*
- *Human resource administrators need to know the information to perform their duties.*
- *Other individuals authorized by the agency (i.e. proxies or delegates, or individuals responsible for generating system reports).*

*Access to information is determined and authorized by the participating agency.*

*In addition, a limited number of system administrators who have been cleared through the Treasury background investigation process and cleared by OPM will have direct access to employee data and data that result from actions taken in each agency portal. This does not necessarily mean that the system administrator will access the data, but it will be accessible to them when they perform their oversight functions. Any actual viewing of the information only occurs if necessary in the performance of their duties.*

*Access is granted based upon need. Individuals with elevated access to information must complete a security authorization form signed by an authorized agent of their agency and be approved by the inCompass program prior to having access granted.*

*Access is restricted based upon need to perform duties for a given agency and given segment of the population. Access is also restricted to a given HR program or business process as necessary to meet need to know limitations..*

### 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?

*The inCompass program has an Information Security Agreement (ISA) with HRConnect that addresses the system connections and security for the data transfers. Additionally, each individual granted access above basic end-user privileges signs a security form with rules of behavior, which dictate the individual's behavior when using the data in inCompass. Rules of behavior must be accepted by users before they are granted access.*

*Treasury EBS offers CSOD to other agencies via a blanket purchase agreement. As stated earlier, each agency has their own portal with their own data, and data is not shared across participating agency portals. Security roles are determined by the participating agency and are consistent with Treasury security governance, Federal Information Security Management Act (FISMA), and Federal Risk and Authorization Management Program (FedRAMP) as guideposts.*

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

### External Information Sharing

**Section 5.4(a)** ☐ Yes ☒ No Is PII maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?

*Neither CSOD nor the inCompass program share information with external entities (e.g., NFC). Treasury EBS offers CSOD to other agencies via a blanket purchase agreement. Each agency has their own portal with their own data, and data is not shared across portals. Security roles are determined by the agency with Treasury security governance, FISMA, and FedRAMP as guideposts.*

*CSOD sends data back to HRConnect, which sends Enterprise Human Resources Integration training data to OPM for the following agencies: USAID and HUD.*

## 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?

*Neither CSOD nor the inCompass program share information with external entities unless artifacts from the system are used in employment related actions. Treasury EBS offers CSOD to other agencies via a blanket purchase agreement. Each agency has their own portal with their own data, and data is not shared across portals.*

*CSOD sends data back to HRConnect, which sends Enterprise Human Resources Integration training data to OPM for the following agencies: USAID and HUD.*

## 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)?

*No additional statutes or regulations restrict disclosure of any of the PII in the system.*

## 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?

*Neither CSOD nor the inCompass program share information with external entities unless artifacts from the system are used in employment related actions. The inCompass program does not have an MOU with any external agencies, organizations, or individuals.*

## 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? |
| *inCompass does not have any MOUs that limit or place conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII.* |

## 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? |
| *No MOUs are required because no PII from this system is currently shared externally. Neither CSOD nor the inCompass program share information with external entities unless artifacts from the system are used in employment related actions.* |

## External Information Sharing Chart

| |
|---|
| **Section 5.4(k)** ☐ Yes ☒ No Is information from the system or project shared externally?<br><br>*PII from the system is not currently shared from inCompass, but it is possible that PII from the system will be shared with external entities if artifacts from the system are used in employment related actions. This PCLIA will be updated to identify those external agencies if and when this occurs.* |

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

| |
|---|
| **Section 5.4(l)** ☐ Yes ☐ No ☒ N/A Is the individual's consent obtained, where feasible and appropriate, prior to any **new** disclosures of previously collected records in a system of records (those not expressly authorized by the Privacy Act or contained in the published SORN (e.g., in the routine uses))? |
| *Neither CSOD nor the inCompass program share information with external entities unless artifacts from the system are used in employment related actions. CSOD participating agencies (including the Treasury inCompass program) only disclose information within the participating agency. Any external disclosures of this information are made by other internal agency systems with which PII from CSOD is shared in accordance with relevant systems of records notices.* |

# Section 6: Compliance with federal information management requirements

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

## Section 6.1: Privacy Act System of Records Notice (SORN)

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

**System of Records**

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

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

*Data may be reviewed in CSOD through the user interface after authentication to the system. The user interface supports both user information and reports.*

*The following classes of users will have some type of rights to view the individual's information on a limited basis:*

- *The employee*
- *The employee's supervisor and superiors within their chain of command*
- *Human resource administrators*
- *Other individuals authorized by the agency (i.e. proxies or delegates, or individuals responsible for generating system reports).*

*Individuals with elevated access to information within each agency's portals must complete a security authorization form signed by an authorized agent of their agency and be approved by the inCompass program prior to having access granted.*

*This system operates under the SORN, OPM/GOVT-1, General Personnel Records, https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/html/2012-29777.htm*

## 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?

*Neither CSOD nor the inCompass program collect any information directly from non-government personnel. .*

## 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 approve a retention schedule for the records maintained in the system or by the project?

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

*The system will comply with federal records retention standards as determined by NARA. The applicable NARA GRS include GRS XX.*

Learning records generally: GRS 2.6,
https://www.archives.gov/files/records-mgmt/grs/grs02-6.pdf

Learning records (specifically individual development plans): GRS 2.6, item no. 030

Workforce and succession planning records, GRS 2.2, item no. 020
https://www.archives.gov/files/records-mgmt/grs/grs02-2.pdf

Employee performance records, GRS 2.2, item nos. 070-073

Hiring records generally: GRS 2.1,
https://www.archives.gov/files/records-mgmt/grs/grs02-1.pdf

Pre-employment (including vetting and background investigation) records: GRS 2.1, item nos. 140-143

Employee awards records, GRS 2.2, item 030
https://www.archives.gov/files/records-mgmt/grs/grs02-2.pdf

- This schedule does not apply to agency-level awards. System users who plan to issue agency-wide awards identify an agency-specific records retention schedule.

## 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 system was granted an ATO effective September 15, 2018.*

## 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 following are controls in place to protect data from unauthorized access:*

- *separate portals for each agency*
- *password management*
- *chain-of-command access controls*
- *closely controlled administrative accounts*
- *account audits, including inactive account cleanup*
- *role-based intra-system access control*

*The following classes of users will have some type of rights to view reports, based on defined permissions and constraints:*

- *The employee has access to their own information*
- *The employee's supervisor and superiors within their chain of command*
- *Human resource administrators*
- *Other individuals authorized by the agency (i.e. proxies or delegates, or individuals responsible for generating system reports)*

*Access to information is determined and authorized by the agency.*

*The reports will be used to:*

- *Manage and create effective Human Capital Strategies;*
- *Monitor and improve HR programs;*
- *Track and report information required by federal law, federal standards and organizational policy.*

*inCompass Program, EBS Security, agency HR program administrators, agency system administrators, and agency security officers are responsible for protecting the privacy rights of the public and employees affected by the interface.*

*CSOD staff are involved with the design and development of the system and EBS contractors are involved with front-end application configuration and day to day operations and maintenance of the system.*

## 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)?

*The agency using inCompass is ultimately responsible for the state of their data. inCompass does a review of all security requests, as noted above, to mitigate any additional risks.*

## Security Controls When Sharing Internally or Externally

**Section 6.4(e)** ☒ Yes ☐ No ☒ N/A Are all Treasury/bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system to internal or external parties?

*The HRConnect border server resides on the HRConnect General Services System (GSS) that is connected to the Department of Treasury's Network (TNet) Wide Area Network (WAN). The vendor provides the infrastructure platform in the Equinix El Segundo, California hosting facility. This is a two-way connection; data flows from HRConnect to and from the vendor although all connections are initiated by HRConnect border server.*

*HRConnect, via automatic processes, uses Secure File Transfer Protocol (SFTP) from the HRConnect border server to logon to the vendor infrastructure, securely encrypt and transmit the file back to the HRConnect border server. The vendor provides the service used to facilitate data transfer. Data extracts destined for HRConnect and WARS are placed securely on the vendor SFTP server where HRConnect will automatically retrieve them. The security of the information being passed from this connection is protected through the use of Federal Information Processing Standards Publication (FIPS) 140-2 approved encryption mechanisms. The connections at each end are located within controlled access facilities. All access is controlled by authentication methods and is role-based to validate approved users.*

*The vendor and Treasury firewalls serve as the primary access control mechanisms between entities. The type of communications established between HRConnect and the vendor consists of data feeds through an outbound encrypted SFTP connection established from HRConnect's border server to the vendor's SFTP server prior to a data transfer. Once the connection is established, the vendor and HRConnect border servers can authenticate and transfer data via SFTP. Treasury will always initiate this connection and either place Pretty Good Privacy (PGP) encrypted data or retrieve it. This connection is intended for bulk data transfers.*

## 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?

*The system captures employee work locations at the Geographic Location Code level (Country / State / City / County). The system has no ability to track employee locations more specifically.*

*The system can identify and locate individuals based on their work location and track their activities in the system. The system has no capacity to determine where any given employee is in real time, based on GPS or any other tracking technology.*

## 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?

*Audit history can be requested from CSOD as needed.*

*Activities happening in CSOD that create data records include the following:*

- *Training attendance / completion tracking*
- *Performance goals and assessment of progress toward those goals*
- *Individual goals aligned with organizational goals or strategies*
- *Competency assessment results*
- *Self-disclosed resume data*
- *Annual award amounts*
- *Certification tracking and progress toward maintaining / acquiring certification*
- *Current and previously held positions*
- *Self-disclosed career interests*

*Access to the system and the underlying data warehouse is protected from unauthorized access and modifications via the use of firewalls, intrusion detection devices, role-based access control polices, auditing, etc. as described in the vendor and Treasury inCompass system security plans.*

*Data may be reviewed in CSOD through the user interface after authentication to the system. The user interface supports both user information and reports.*

*The following classes of users will have some type of rights to view the individual's information on a limited basis:*

- *The employee*
- *The employee's supervisor and superiors within their chain of command*
- *Human resource administrators*
- *Other individuals authorized by the agency (i.e. proxies or delegates, or individuals responsible for generating system reports)*

*Individuals with elevated access to information within each agency's portals must complete a security authorization form signed by an authorized agent of their agency and be approved by the inCompass program prior to having access granted.*

## 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?

*The system vendor provides and maintains a Voluntary Product Accessibility Template (VPAT) certification Additionally, if a 508 issue is found, it will be escalated and resolved to as a Priority 1 issue (i.e., a high priority issue requiring immediate resolution).*

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

## Additional Redress Mechanisms

| |
|---|
| **Section 7.0(c)** ☒ Yes ☐ No With respect to information maintained by the project or system (whether or not it is covered by the Privacy Act), does the bureau or office that owns the project or system have any additional mechanisms other than Privacy Act and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)? |
| *The participating agency using CSOD is ultimately responsible for the state of their data.*<br><br>*Users may review and provide feedback on the accuracy of the data in the system to the appropriate participating agency personnel.*<br><br>*With an automated data feed, if there are errors, an error report is generated each night the HR Connect feed runs, specifically identifying errors that prevent the system from updating core user information. When a manual feed is run, if there are errors, the error reports generate upon completion of the upload. The error report identities the issue and allows for correction of the data from the source system before the next feed occurs. This data correction process is inherited from HRConnect.*<br><br>*Additionally, each agency's human resources program office is responsible for testing the configured business process and workflow to ensure accurate and desired results are achieved. If there is an error, it is the responsibility of the participating agency's process owner to take appropriate steps to correct the findings.* |