Appendix C: Privacy and Civil Liberties Impact Assessment Template

Privacy and Civil Liberties Impact Assessment
for the

Integrated Talent Management System

January 17, 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 is being conducted for the Integrated Talent Management (ITM) System for the first time. A PCLIA was previously completed for the Treasury Learning Management System (TLMS) and the Electronic Learning Management System (ELMS) predecessor systems that performed some of the functions now consolidated under ITM.

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

The purpose of the ITM is to provide the Department of the Treasury enterprise integrated talent management solution that provides the following functions:

- ***Competency Management***: Identifying and developing human capacity based upon knowledge, skills and ability.
- ***Learning Management***: Delivering and managing training targeted to each member of an organization.
- ***Succession and Development Planning***: Identifying (and developing) members with the potential to fill key positions.
- ***Performance Management***: Aligning member achievement with an organization's goals and expectations.
- ***Workforce Planning***: Aligning the needs and priorities of an organization and its workforce to meet objectives.
- ***Analytics***: Integrating and reporting data to create a real-time, vibrant view of the workforce.

ITM uses PII to provide Department of the Treasury employees and contractors with unique accounts and credentials and to facilitate reporting required by the Office of Personnel Management (OPM). ITM supports the Treasury mission by reducing costs, retiring over 20

existing talent management systems and replacing them with a single enterprise solution. Most significantly, ITM will consolidate the existing IRS Electronic Learning Management System (ELMS) and Treasury Learning Management System (TLMS) into a single system. Long term, the intent is for ITM to support other agencies as part of a cross-services initiative.

This PCLIA will be updated as the project moves forward if new PII risks are identified. The vendor's Secure Fed and Civilian Node with Human Capital Management (HCM) Suite system provides a means through which employees may identify, manage, and perform talent management activities, such as completing their training requirements, annual performance planning, and competency assessments. It also permits managing and administering Treasury's talent management programs.

Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project		
☐ **0 – 999**	☐ **1000 – 9,999**	☐ **10,000 – 99,999**
☒ **100,000 – 499,999**	☐ **500,000 – 999,999**	☐ **1,000,000+**

Section 3.2: Authority to Collect

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

5 U.S.C. § 301- *Departmental regulations* – regulations for the operation of the department; conduct of its 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 authorities of the Secretary of the Treasury*.
- 44 U.S.C. § 3554, *Federal Information Security Modernization Act (FISMA)* - instructs the head of each federal agency to provide, "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."
- 44 U.S.C. 3534, *Federal agency responsibilities* – agency responsibilities for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruptions, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
- 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.
- OMB Circular A-130, Appendix I, Management and Protecting Federal Information Resources.

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 conditions5 U.S.C. §552a (k). The proposed exemption must be described in a Notice of Proposed Rulemaking ("NPRM"). In the context of the Privacy Act, the purpose of the NPRM is to give the public notice of a Privacy Act exemption claimed for a system of records and solicit public opinion on the proposed exemption. After addressing any public concerns raised in response to the NPRM, the agency must issue a Final Rule. It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final Rule process.

Section 4.1(a) Please check all of the following that are true:

1. ☐ None of the PII maintained in the system or by the project is part of a Privacy Act system of records;
2. ☒ All of the PII maintained in the system or by the project is part of a system of records and none of it is exempt from the Privacy Act relevant and necessary requirement;
3. ☐ All of the PII maintained in the system or by the project is part of a system of records and all of it is exempt from the Privacy Act relevant and necessary requirement;
4. ☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and the records to which the Privacy Act applies are exempt from the relevant and necessary requirement; and

☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and none of the records to which the Privacy Act applies are exempt from the relevant and necessary requirement.

Section 4.1(b) ☒ Yes ☐ No ☐ N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, was an assessment conducted prior to collection (e.g., during Paperwork Reduction Act analysis) to determine which PII types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements?

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

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

The records in this system of records are covered by the OPM/GOVT-1, General Personnel Records, and system of records notice (SORN). None of the records in this government wide SORN are exempt from the relevant and necessary requirement under the Privacy Act. The Office of Privacy, Transparency, and Records (PTR) evaluated the collection of limited information from Treasury employees and contractors and determined that the limited information is both relevant and necessary to carry out the mission of the ITM.

Section 4.2: PII and/or information types or groupings

To perform their various missions, federal agencies must necessarily collect various types of information. The checked boxes below represent the types of information maintained in the system or by the project. Information identified below is used by the system or project to fulfill the purpose stated in Section 3.3 – 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
☐ Sexual Orientation	☐ User names, avatars etc.	☐ 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): *Job Title*
☐ ☒ Other (please describe): *Work experience*	☐ Other (please describe): _____	☐ Other (please describe): _____

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

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

Medical/Emergency Information Regarding Individuals		
☐ 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
☐ Information provided under a confidentiality agreement	☐ Information subject to the terms of an international or other agreement	☐ Other (please describe): _____

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: _____	☐ Other (please describe: _____
☐ Other (please describe: _____	☐ Other (please describe: _____

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

HR Connect	End User
Specific PII identified in Section 4.2 that was acquired from this source: *- Name* *- Date of Birth* *- Business Email Address* *- Full Social Security Number* *- Employee Identification Number* *- Business Physical/Postal Mailing Address* *- Job Title*	**Specific PII identified in Section 4.2 that was acquired from this source:** *- Education Information* *- Resume and curriculum vitae* *- Group / Organization Membership* *- Personnel Files (Performance Appraisals)* *- Personal Home Phone Number or Fax* *- Business Phone Number or Fax* *- Personal Cell Phone Number* *- Zip Code* *- Military Service Information* *- Citizenship* *- Personal Email Address* *- Professional / personal references* *- Home Physical / Postal Mailing Address* *- Work experience*
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
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.
☐ 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
☐ Email	☐ Email
☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.
☒ Bulk transfer	☐ 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).
☐ 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
☒ Other: Please describe: *Transmitted daily via a core data feed with HR Connect.*	☒ Other: Please describe: *Employees are provided the option to enter, if they so choose, details specific to their professional / educational experience and professional affliations to a resume / profile function within ITM. These voluntary fields are populated by the employee; edits and updates are tracked via system audit capabilities.*
☐ Other: Please describe: _____	☐ 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.

PII is collect and maintained only through a daily core data feed from HR Connect. Individuals can opt to provide PII as it relates to their professional / educational experience and professional affiliations. Additionally, ITM facilitates the Treasury performance management processes. As such, it collects personnel information related to employee performance from employees and supervisors. HR Connect data are, however, collected directly from employees.

Treasury employees and contractors are notified every time they log onto their Treasury issued computers that their transactions on government devices are not private and are subject to review.

Use of Social Security Numbers

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

In addition, the Privacy Act provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *Id.* at § 7(a)(2)(A)-(B).

Section 4.4(d) ☒ Yes ☐ No ☐ N/A Does the system or project maintain SSNs?

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

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

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

☐ The SSN is disclosed to any Federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *If checked, please provide the name of the system of records in the space provided below.*

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

SSNs and dates of birth are required for mandatory OPM Enterprise Human Resources Integration (EHRI) reporting. No other unique identifiers are acceptable. Additionally, because SSNs are collected via an integration with HR Connect, there is not a point of manual entry / collection during which individuals would be asked about disclosure.

First Amendment Activities

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

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

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

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

☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.

☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity.

☐ There is a statute that expressly authorizes its collection.

☐ N/A, the system or project does not maintain any information describing how any individual exercises their rights guaranteed by the First Amendment.

ITM does not collect or maintain any information describing how an individual exercises their rights guaranteed by the First Amendment. Therefore, no associated 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.

The purpose of the Integrated Talent Management (ITM) system is to provide employees, their supervisors, human resources, and training departments more efficient means to manage every aspect of the human resource management functions by leveraging the Systems, Applications & Products in Data Processing and Software as a Service (Saas) which is hosted externally by the vendor cloud offering. The function of the system is to provide the leading SaaS offering for HCM that conforms to the stringent guidelines and requirements established under the Federal Risk and Authorization Management Program (FedRAMP). The vendor SaaS delivers a comprehensive suite of solutions that improves executive insight and decision-making while ensuring the right people with the right skills are doing the right work. This is enabled through a tightly integrated solution suite, which delivers capabilities that ensure organizations can manage the full lifecycle of the employee to include:

- *Performance and Goals Management*
- *Compensation Management*
- *Succession and Development*
- *Learning*
- *Workforce Planning*
- *Workforce Analytics and Reporting*

As noted in Section 4.2, ITM also collects and maintains some PII. This data is collected and maintained via a nightly data feed from HR Connect to ITM. This ensures that ITM data is accurate, timely, and maintained only by the HR system of record. Additionally, data collected by ITM is not transparent / accessible by end-users unless they have been granted administrator access / permissions. As a result, ITM ensures there are no deviations or alterations of data collected beyond what is readily available in HR Connect; i.e. official Treasury email addresses. Specifically:

- *First Name, Last Name, Business Email Address, Employee ID, Business Physical Address, Job Title, & Manager are collected for the purposes of creating a unique user record. This user record provides the unique information needed to link system actions, such as completing training, to Treasury employees and contractors*
- *As desired, employees can also enter resume / curriculum vitae into the system which may include: group / organization membership, personal home phone number or fax, business phone number or fax, personal cell phone number, zip code, military service information, citizenship, personal email address, professional / personal references, home physical / postal mailing address, work experience, and education information into ITM.*
- *Additionally, and specifically for the business use of transmitting required EHRI to OPM, the collection of both full social security numbers and dates of birth is required. The vendor, is contractually obligated for accurately delivering this reporting directly to OPM. Previous precedent exists for both TLMS & ELMS, which are previous versions of the Learning Module within the Talent Management Suite.*
- *Lastly, ITM will facilitate the annual performance management processes for the Department of the Treasury. As such, it will store some data related to employee performance/personnel files. This data will be collected in system configured tasks; completed by the employee and reviewers involved in the performance management process (rating officials, reviewing officials, etc.). Upon completion of the annual performance cycle, final employee ratings will be encrypted and placed on the border server (a treasury sever which facilitates the secure placement and pushing of data between systems) for collection by HR Connect.*

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

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

Section 5.1(a) ☒ Yes ☐ No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination about an individual's rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)? **Section 5.1(b)** ☒ Yes ☐ No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual's rights, benefits, and privileges under federal programs? **Section 5.1(c)** ☒ Yes ☐ No ☐ N/A If information could potentially be used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs, does the system or project collect information (to the greatest extent practicable) directly from the individual?
The ITM will contain employee training transcripts, performance appraisals, competency assessments, and other data that, in unique and specific cases, could be used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs. For instance, delinquent performance and mandatory training completions could result in corrective actions against the employee.

Data Mining

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

Section 5.1(d) ☐ Yes ☒ No Is information maintained in the system or by the project used to conduct "data-mining" activities as that term is defined in the Implementing the 9-11 Commission Act?
No privacy and civil liberties risks have been identified because ITM does not perform any "data mining" activities covered by the Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3 (b)(1)(C)(ii).

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?

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

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

Section 5.2(e) ☐ Yes ☐ No ☒ N/A Does the bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings, or obtain Data Integrity Board approval in accordance with Section (p) of the Privacy Act before taking adverse action against the individual?

ITM does not maintain information used as part of a matching program or a system of records. 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?
The collected data is verified for accuracy, relevancy, and completeness by the employees who submit their information to the Department of the Treasury. Employees are given an opportunity to amend or explain their information in the system 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?
ITM does not merge data with another system, but data will be shared with selected systems. Internally, HR Connect will receive annual performance ratings and Enterprise Data Management (EDM) Workforce Analytics will receive talent management data to drive enterprise reporting. Externally, ITM will send mandatory reporting data to OPM EHRI.

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)?
Performance ratings and performance awards will be generated in ITM and transmitted / uploaded into the HCM application in HR Connect, from which point they are passed to the National Finance Center (NFC) which maintains the official HR record. The NFC is responsible for reporting to OPM EHRI data warehouse and electronic Official Personnel Folder (eOPF).

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 are collected either via the nightly core data feed with HR Connect, or from end user actions when they use particular system features and functions. HR data imported into the system from HR Connect ensure the accuracy of PII within ITM; matching and updating records as needed based on the Employee ID. End users and system administrators may review and provide feedback on the accuracy of the data in the system. PII collected by ITM is either received via the HR Connect data feed, and thus it is the responsibility of HR Connect and business owners to ensure the data provided is correct. Because the data feed runs nightly, any corrections made to HR Connect will be reflected in ITM the following day.

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?

PII collected by ITM is either received via the HR Connect data feed, and thus it is the responsibility of HR Connect and business owners to ensure the data provided is corrected when needed. Because the data feed runs nightly, any corrections made to HR Connect will be reflected in ITM the following day.

Additionally, with specific and limited exceptions, end users can enter education information and resume details within ITM. It is the individual's responsibility to maintain and correct these details, as the data is not collected and received any other way.

The system maintains PII related to performance ratings and performance awards generated within the ITM. While ITM is the place where performance plans are initiated and closed out, ITM is not the official repository for performance management information. Once annual performance rating and award tasks are completed, the information is pushed to HR Connect for internal record keeping. This data push is not an automated or ongoing feed, and make corrections to the data sent to HR Connect. For award, HR Connect alone sends the final performance rating and award details to NFC.

In cases, where changes need to be made to the performance rating and award details captured within the ITM. Performance and award actions need to be reopened, and a request for an exception to push the corrections will be submitted and processed.

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")?

PII is provided by HR Connect to ITM and reported back to HR Connect by ITM in other cases. Additionally, system reporting within the ITM is deliberately separated by bureau.

The following classes of users will have some type of rights to access data in the system through reports, or the employee profile information, determined by system enforced defined permissions and constraints. Please note, as a requirement of ITM access, bureaus are limited to accessing their own data.

- *The employee has access to their own information.*
- *The employee's supervisor and superiors within their chain of command because they have a need to know the information to perform their supervisory duties.*
- *Human Resource Administrators who have a need to know the information.*
- *Other individuals authorized by the bureau (i.e. proxies or delegates, or individuals responsible for generating system reports).*
- *If the employee expressly authorizes the sharing of their PII (e.g., if the employee accepts a position in a different Treasury bureau).*

In addition, a limited number of system administrators who have been cleared through the Treasury background investigation process and OPM will have direct access to employee data and data that result from actions taken in each client 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 their manager, bureau administrator and the system owner prior to having access granted.

Access will be restricted based upon need to perform duties for a given organization and given segment of the population, and even restricted to a given Human Resources program or business process.

Memorandum of Understanding/Other Agreements Limiting Treasury's Internal Use/Disclosure of PII

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

There are no MOUs and other agreements limiting Treasury's internal use or disclosure of PII.

Internal Disclosures

The ITM shares and reports mandatory reporting data to OPM EHRI and transmits annual employee performance ratings to HR Connect for record retention and the processing of performance based awards. The ITM application / program does not share information with any other external entities beyond these two intra-agency disclosures.

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 Treasury ITM system security plan. System error logs and emails do not contain PII, and are restricted to Treasury users.

Data may be reviewed in ITM 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 bureau; i.e. proxies or delegates, or individuals responsible for generating system reports.*

Individuals with elevated access to information must complete a security authorization form signed by their manager, bureau administrator and the system owner prior to receiving.

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?

As mentioned in previous sections, 3.1/4.2/5.1, ITM requires SSNs and dates of birth to facilitate the reporting of mandatory training data to OPM EHRI. As unique identifiers, these values are required to update individual records maintained by OPM.

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?

The ITM shares and reports mandatory reporting data to OPM EHRI. The ITM application / program does not share information with any other external entities.

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)?

Treasury is not bound by any MOU or other agreement in its use of any of the information 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?
Treasury has not executed any MOU or other agreement with OPM. The information sharing is required by law.

Memorandum of Understanding Limiting Treasury's Use or Disclosure of PII

Section 5.4(i) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency, an international agreement or treaty, or contract with private vendor that provided the information to Treasury or one of its bureaus) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII?
Treasury is not bound by any MOU or other agreement in its use of any of the information in the system.

Memorandum of Understanding Limiting External Party's Use or Disclosure of PII

Section 5.4(j) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party's use, maintenance, handling, or disclosure of PII shared by Treasury?
Treasury has not executed any MOU or other agreement with OPM. The information sharing is required by law.

External Information Sharing Chart

Section 5.4(k) ☒ Yes ☐ No Is information from the system or project shared externally?			
External Recipient's Name	*OPM EHRI*	N/A	N/A
Purpose of the Sharing PII Shared	*To meet mandatory reporting requirements on employee training data to OPM.*	N/A	N/A
Content of Applicable Routine Use/Citation to the SORN	80 FR 75785	N/A	N/A
Applicable Statutory or Regulatory or Restrictions on Information Shared	*5 CFR 337* *5 CFR 576* *5 CFR 792* *5 CFR 831* *5 CFR 842*	N/A	N/A
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Source/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of PII)	*An ISA will be established to facilitate this process.*	N/A	N/A
Name and Description of Relevant MOUs or Other Agreements Containing Restrictions Imposed by Treasury on External	*An ISA will be established to facilitate this process.*	N/A	N/A

Sharing Partner (including description of restrictions imposed on use, maintenance, and disclosure of PII)			
Method(s) Used to Transfer PII (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other)	*On a monthly basis, the required EHRI data will be encrypted and pushed to the Treasury Border Server, and then pushed to OPM EHRI to satisfy the reporting needs.*	N/A	N/A
Per section 5.1, ITM will need to share/submit some PII to OPM EHRI to satisfy mandatory reporting requirements.			

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))?
ITM reports mandatory data to OPM EHRI and transmits annual employee performance ratings to HR Connect for record retention and the processing of performance based awards. ITM does not share information with any other external entities beyond these two intra-agency disclosures.

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 ITM 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 bureau; i.e. proxies or delegates, or individuals responsible for generating system reports.*

Individuals with elevated access to information must complete a security authorization form signed by their manager, bureau administrator and the system owner prior to having access granted. All access is based on need to know.

This system operates under the System of Record Notice OPM/GOVT-1, General Personnel Records, (https://www.opm.gov/fedregis/2006/71-061906-35363-a.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?
ITM does maintain information on Treasury contractors, but only information necessary to determine whether they completed contractually required training. ITM receives from HR Connect a daily data feed of information regarding these contractors who are contractually required to take particular training. ITM does not actually collect any information from these contractors. All collection is done by HR 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 approved a retention schedule for the records maintained in the system or by the project?

Section 6.3(c) ☐ Yes ☐ No ☒ N/A If NARA did not approve a retention schedule for the records maintained in the system or by the project and the records are not covered by NARA's GRS or Treasury/bureau SRS, has a draft retention schedule (approved by all applicable Treasury and/or Bureau officials) been developed for the records used in this project or system?
The system will comply with federal records retention standards as determined by NARA. The applicable NARA General Records Schedules include GRS 2.2 and GRS 2.6.

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 ITM is subject to FISMA requirements and has been designated as moderate. At the samer time this PCLIA was being developed, a Security Assessment and Authorization (SA&A) was completed along with supplemental documentation. The Authorization to Operate (ATO) was signed and SA&A was received on January 9, 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?
Only authorized Treasury employees and contractors with proper authorization will have access to data. *The following are controls in place to protect data from unauthorized access:* • *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 Departmetn of the Treasury* *Access to information is determined by the organization and is documented on the Security Authorization form.* *The reports will be used to:* • *Manage and create effective Human Capital strategies;* • *Monitor and improve Human Resource programs;* • *Track and report information required by federal law, federal standards and Treasury policy.*
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)?

A potential risk has been identified with regards to details entered by the end user. It is possible an invidiual could choose to enter information beyond what is intended in open text fields. To mitigate this issue, administrations will run regular reports on data entered by the end user to identify any deviances from the intended use of the resume portion of the system. As identified, employees will be notified to correct remove PII that should not be within ITM.

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?

Description of Connection. The benefit of the interconnection is to automatically transmit talent management data from ITM to Treasury HR Connect and OPM EHRI.
The HR Connect border server resides on the Department of the Treasury's Network (TNet) Wide Area Network (WAN). The Vendor provides the infrastructure platform in the Herndon, VA hosting facility.

This is a two-way connection; data flows from HR Connect to and from the vendor although all connections are initiated by HR Connect Border Server.

HR Connect, via automatic processes, uses Secure File Transfer Protocol (SFTP) from the HR Connect Border Server to logon to the vendor infrastructure, securely encrypt and transmit the file back to the HR Connect Border Server. The vendor provides the service used to facilitate data transfer. Data extracts destined to HR Connect are placed securely on the vendor SFTP server where HR Connect 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 HR Connect and the vendor consists of:
Data feed - An outbound encrypted SFTP connection will be established from HR Connect's border server to the vendor's SFTP server prior to a data transfer. Once the connection is established, the vendor and HR Connect 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 captures employee information, like job title, occupational series, salary type, and pay plan, to populate fields in ITM for determining type of training and performance review, etc.

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?

Activities happening in ITM 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, Education, & Professional Affiliation Data*
- *Current and Previous Held Positions*
- *Development Plans and Goals*

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 Treasury ITM system security plan.

Data may be reviewed in ITM 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 bureau; i.e. proxies or delegates, or individuals responsible for generating system reports.*

Individuals with elevated access to information must complete a security authorization form signed by their manager, bureau administrator, and the system owner 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 for the current and subsequent versions of the application. Additionally, if a 508 issue is found, it will be escalated and the vendor will be notified in writing to resolve.

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?
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 data from the ITM and system logs reflect what transpired at a specific time. Users may review and provide feedback on the accuracy of the data in the system to the appropriate agency personnel. *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. This data correction process is inherited from HR Connect. If data integrity issues are observed or errors occur as a result of the HR Connect integration, then the HR Connect program is notified of the issue and works with the appropriate business owners to resolve the issue.* *Additionally, the human resources program office is responsible for testing the configured business process and workflow to ensure accurate and desired results are the achieved. If there is an error, it is the responsibility of the business process owner to take appropriate steps to correct the findings.*