# U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

## Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

**Name of Project:** DOI FedTalent System
**Bureau/Office:** Interior Business Center
**Date:** September 28, 2021
**Point of Contact:**
Name: Danna Mingo
Title: Departmental Offices Associate Privacy Officer
Email: OS_Privacy@ios.doi.gov
Phone: (202) 208-3368
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

## Section 1. General System Information

**A. Is a full PIA required?**

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No:

**B. What is the purpose of the system?**

The Department of the Interior (DOI) FedTalent system is a training and performance management system for its employees in order to execute its mission and meet Federal requirements. Federal personnel, students and other DOI affiliates will access the FedTalent system for the purpose of registering for training courses and completing training. Federal employees and supervisors will also access the FedTalent system for the purpose of employee performance management.

FedTalent is an open-source distribution and extension of Moodle-developed software developed by Totara with a wide range of features to support organizational learning (i.e., mandatory training, eLearning, blended learning, social learning, and classroom training administration), performance management, appraisal, revalidation, team management and report building. The FedTalent System consists of two modules: the Learning Management Module (LMM) and a Performance Management Module (PMM) which are accessible via the web.

The FedTalent LMM provides an integrated learning management solution. DOI has an ongoing need to provide high-quality training to its employees in order to both comply with government regulations and to improve employee engagement. The FedTalent LMM automates the end-to-end workflow process for training requests and completion, thereby, eliminating the manual process and making the records easily manageable by Federal agencies. The LMM allows online access to mandatory, optional, and developmental training. The LMM provides access to a multitude of online courses developed by Skillsoft, DOI's online training provider. The LMM allows DOI to generate training reports for the Office of Personnel Management (OPM) through OPM's Employee Human Resource Integration (EHRI) system.

The FedTalent PMM provides an integrated performance management function that automates the end-to-end workflow process for Federal agencies to manage the annual employee performance review process. The PMM is integrated with the OPM's Electronic Official Personnel Folder (eOPF), and has the capability to generate employee performance reports for OPM.

The DOI Interior Business Center (IBC) Human Resources (HR) Directorate, Human Resources Management Systems Division (HRMSD) is responsible for the operation and maintenance of the FedTalent System. IBC is a designated Human Resources Federal Shared Service provider for DOI and other Federal agency customers, who will utilize the FedTalent system to manage their own training and performance management records.

DOI is an IBC internal customer and will use the FedTalent system to manage employee training and performance records. DOI's instance of FedTalent is re-branded as "DOITalent". This assessment covers DOI's use of DOITalent and the FedTalent system as a shared service offering.

The current instance of DOI Talent has replaced the decommissioned DOI Learn system. The learning histories/transcript data for active DOI employees was transferred to DOI Talent, and data for departed employees and others are stored in a SQL server database hosted on an OCIO SQL server instance. The OS Records Officer and Program Manager will monitor the data in the SQL server database and will annually dispose of records meeting the seven-year retention in accordance with Departmental records policies and procedures.

**C. What is the legal authority?**

5 U.S.C. 4101, et seq., Government Organization and Employee Training; 5 U.S.C. 1302, Regulations; 5 U.S.C. 2951, Reports to the Office of Personnel Management; 5 U.S.C. 4118, Regulations; 5 U.S.C. 4308; 5 U.S.C. 4506, Regulations; 5 U.S.C. 3101, General authority to employ; 5 U.S.C. 1104, Delegation of authority for personnel management; 5 U.S.C. 3321, Competitive service; probationary period; 5 U.S.C. 4305, Regulations; and 5 U.S.C. 5405, Regulations; 43 U.S.C. 1457, Title VI of the Civil Rights Act of 1964 as amended (42 U.S.C. 2000d); 42 U.S.C. 12101, Americans with Disabilities Act of 1990; 44 U.S.C. 3501, et seq.; E-Government Act of 2002 (P. Law 107-347); Executive Order 11348, Providing for Further Training of Government Employees, as amended by Executive Order 12107, Relating to Civil Service Commission and Labor Management in Federal Service; 5 CFR 410, Subpart C, Establishing and Implementing Training Programs; and Office of Management and Budget (OMB) and the United States Office of Personnel Management (OPM) Human Resources Line-Of-Business initiative to migrate United States Government agencies to Federal Human Resources (HR) Shared Service Centers (SSC).

**D. Why is this PIA being completed or modified?**

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

**E. Is this information system registered in CSAM?**

☒ Yes:

010-999991241; FedTalent System Security and Privacy Plan

☐ No

**F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.**

| **Subsystem Name** | **Purpose** | **Contains PII** *(Yes/No)* | **Describe** *If Yes, provide a description.* |
|---|---|---|---|
| None | None | No | N/A |

**G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?**

☒ Yes:

Federal employee training records are covered by OPM/GOVT-1, General Personnel Records, 77 FR 73694 (December 11, 2012); modification published 80 FR 74815 (November 30, 2015). Performance management records are covered under OPM/GOVT-2, Employee Performance File System Records, 71 FR 35347 (June 19, 2006); modification published 80 FR 74815 (November 30, 2015). Department of the Interior (DOI) training records are also maintained under DOI-16, Learning Management System - 83 FR 50682 (October 9, 2018). These notices may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

Each Federal agency customer retains ownership and control over its own records in this system and is responsible for meeting requirements under the Privacy Act for the collection, maintenance and sharing of its records. Individuals seeking information on their records owned and maintained by an agency customer should contact the employing agency in accordance with the applicable agency system of records notices.

☐ No

**H. Does this information system or electronic collection require an OMB Control Number?**

☐ Yes: *Describe*
☒ No

## Section 2. Summary of System Data

**A. What PII will be collected? Indicate all that apply.**

☒ Name
☒ Education Information
☒ Personal Email Address
☒ Employment Information
☒ Other: *Specify the PII collected.*

Learning management records include the First and Last name, official email address, work address, work phone, projected Entry on Duty Date, Primary Email Address, Employee Common Identifier (ECI), Supervisor name and ECI, training records, user profiles, and other information related to training programs for Federal employees and contractors. For non-Federal individuals, the First and Last name, organization, personal email address, and other information may be

collected and maintained to manage the user profile and training records. Training records may include course title, class name, certification requirements met, test scores/transcripts, training requests and acquired skills, payment confirmation from Pay.gov for courses, and vendor information lists.

The Performance Management module only applies to Federal employees. Performance appraisals include employee name, manager and employee work-related performance communications, organization code, position title, GS series, grade level, supervisory status, employee goals, progress (whether favorable or unfavorable), ratings, and work assignments.

The FedTalent system was designed without any fields that would collect or maintain Social Security numbers (SSNs) or Dates of Birth (DOBs) to mitigate risk to individual privacy. DOITalent, the DOI instance of FedTalent, does not contain any processes that require the collection of SSNs or DOB from individuals. However, there is a possibility that supporting documents submitted by individuals for training requests to contain SSNs or other types of PII. Monthly training reports submitted to OPM may include SSN and DOB of Federal employees and this data is extracted from other systems externally from FedTalent for reporting purposes to meet OPM requirements. These OPM training reports in the IBC Datamart system as a record.

Federal employees with PIV cards log into the FedTalent website using their PIV credentials to complete training or performance appraisals. Users who do not have PIV cards will require a User ID and password.

FedTalent is a shared service system and as such provides, as a service to other Federal customer agencies, transmission of monthly training reports to OPM through the EHRI system. These reports may contain various types of PII including name, SSN and DOB to meet OPM's monthly reporting requirements. Each Federal agency customer is responsible their own collection, use, sharing, and dissemination of their data within their instance of FedTalent.

**B. What is the source for the PII collected? Indicate all that apply.**

☒ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☒ Third party source
☐ State agency
☐ Other: *Describe*

There are various data interfaces with internal and external systems including the FPPS and Workforce Transformation Tracking System (WTTS)/Entrance On Duty System (EODS) for the purpose of creating and updating user accounts; migrating learning history information from

legacy systems; facilitating delivery of courses and course completion status with the Skillsoft vendor; processing payments through the Department of the Treasury, Bureau of Fiscal Service Pay.gov website; and submitting training and performance management reports to the OPM EHRI and eOPF.

There are multiple methods for creating accounts for individual FedTalent users. Due to the fact that multiple customer agencies have different needs, FedTalent functionality will be variously configured to meet the needs of each customer agency. The first method is manual self-registration. Those customer agencies that select this feature choose to allow any member of the general public to create a FedTalent user account. Another method is manual account creation by a FedTalent application administrator. For customer agencies that adopt this functionality, the prospective user must complete a user account request form that denotes the username and security level that will be assigned to the user. There is also an automated process called 'HR Import' which interfaces with FPPS Datamart and runs as a nightly batch process. There is also an automated provisioning of FedTalent accounts via the Workforce Transformation Tracking System (WTTS). During the onboarding process an account is created for employees to complete required new hire training. A manual upload of spreadsheet data by a FedTalent application administrator may also be utilized. The system can also be configured to automatically provision user accounts via the DOI ADFS interface using Single Sign-On functionality.

**C. How will the information be collected? Indicate all that apply.**

☒ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*
☒ Other: *Describe*

Federal employees with PIV cards can login into the FedTalent website using their government issued PIV card to complete training or performance appraisals. FedTalent system forwards a request for authentication to ADFS and DOI AD user credentials (federal employees and contractors) are used for authentication purposes.

Users who do not have PIV cards would have to access FedTalent using a standard User ID and Password. DOI affiliates and students would have to provide their names to create a user id and password.

Federal Personnel Payroll System (FPPS): User profiles from FPPS including performance ratings and awards program are used to create and update employee accounts in FedTalent. New

employee accounts are created during the onboarding process, and all new employees must complete mandatory training.

FedTalent users are redirected from the FedTalent website to the Department of Treasury's Pay.gov website to make payments for training courses. Users can also complete an online form hosted by Pay.gov then directed to a collections page upon completing the form. An end-user may also receive an electronic bill, sent by Pay.gov on behalf of FedTalent system, which directs the user to a Pay.gov collection page. A batch file is sent for processing through Pay.gov using Pay.gov's secure batch interface. The batch file received from Pay.gov consists of accounting and financial data which will be forwarded to the DOI Financial and Business Management System (FBMS) for payment processing. Only a confirmation receipt of payment is returned from Pay.gov to the FedTalent system, which includes information such as merchant confirmation number.

User course completion results and score reports are received from Skillsoft, DOI's online training vendor.

**D. What is the intended use of the PII collected?**

The primary purpose for collecting PII is to create user accounts in DOI FedTalent system to process personnel training and performance management actions in order to assist DOI fulfill OPM training and performance recordkeeping and reporting requirements. An individual's PII is collected during the DOI employee onboarding process, and the minimum required is used to establish employee accounts in the FedTalent system. All users without government issued PIV card are required to complete a user account request form.

**E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.**

☒ Within the Bureau/Office:

Data is protected on the basis of the least privilege principles. Individual employees have access to their own training and performance information. Individual employees do not have access to the data pertaining to other employees unless they are in a direct supervisory position for the related employees. Access to performance and training information for a given employee is restricted to their individual Supervisor only. Employees may not view the data which pertains to other employees.

☒ Other Bureaus/Offices:

DOI OCIO Database Administrators will have access to data within the system for system support activities. IBC Help Desk personnel have access to the system for the purpose of assisting customers. FedTalent data flows into FPPS (Datamart) for Rating of Record and Training records to include PII data such as Last Name, First Name, Middle Name, Work Email

Address, Supervisor Last Name, Supervisor First Name, Supervisor Middle Name. Performance rating and awards records will be uploaded to FPPS.

☒ Other Federal Agencies:

Records are shared with OPM, Treasury Department, and other agencies or persons as authorized, consistent with the purpose of the activity and the uses permitted under the Privacy Act and OPM/GOVT-1, General Personnel Records, 77 FR 73694 (December 11, 2012); modification published 80 FR 74815 (November 30, 2015); and OPM/GOVT-2, Employee Performance File System Records, 71 FR 35347 (June 19, 2006); modification published 80 FR 74815 (November 30, 2015). DOI training records are also maintained under DOI-16, Learning Management System - 83 FR 50682 (October 9, 2018). These notices may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn. Reports are submitted to OPM on a monthly basis that include DOI records and records of employees of Federal agency customers. Federal agency customers have access to the data for their own employees that is hosted or processed by IBC.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Information may be shared with Tribal, state or local agencies with individual or student consent or as authorized under the routine use identified in the DOI-16: DOI Learn SORN.

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors will participate in the design, development and updates of the system and will be involved with maintenance of the system. FAR Privacy Act clauses were included in the contract.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Training is also provided by approved vendors such as Skillsoft, a DOI vendor that provides online training courses to employees. Employees can register for and complete online training courses provided by Skillsoft. Course requests are sent to Skillsoft that include employee first and last name, username for authentication and API communications, and asset metadata requests for course import to FedTalent, for the purpose of registering, completing the online course and issuing a certification of completion.

**F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?**

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Information is collected as a condition of employment, and the provision of personal information is provided voluntarily. Individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII during the application and onboarding process. Federal employees and contractors have access to FedTalent system to complete their training and performance management requirements to meet OPM training and performance mandates. Employees may opt to not access the system or complete mandatory training or meet performance management requirements, however, this may have have a negative impact on them in their roles or status as employees.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

**G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is posted on the FedTalent login screen and is available to all users who access the system.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this PIA and published systems of records notices including OPM/GOVT-1, General Personnel Records, 77 FR 73694 (December 11, 2012); modification published 80 FR 74815 (November 30, 2015), OPM/GOVT-2, Employee Performance File System Records, 71 FR 35347 (June 19, 2006); modification published 80 FR 74815 (November 30, 2015), and DOI-16, Learning Management System - 83 FR 50682 (October 9, 2018), which may be viewed at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

Users are provided with a privacy and security warning banner when accessing the system.

☐ None

**H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).**

For the purpose of rating employee performance, FedTalent supervisors might retrieve information on an employee's Annual Performance Rating or employee training information, such as name, username, and other keywords.

**I. Will reports be produced on individuals?**

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports will be produced on individuals for the purpose of completing standard Human Resource Management activities such as Training Management and Performance Management. Only users assigned the permission to create reports via an administrative role can create them. Reports in FedTalent have controls that enable reports administrators to tailor the content to the person running the report (e.g., a supervisor with ability to run a report on their team members' mandatory training progress will see data regarding only those people). Administrators can control who has access to run specific reports based upon system roles (e.g., learners (basic role), supervisors, other admins), as well as on position and/or organization.

☐ No

## Section 3. Attributes of System Data

**A. How will data collected from sources other than DOI records be verified for accuracy?**

Data related to training requests, course registration and performance appraisals is generally manually entered by DOI employees and supervisors and relies upon the responsible parties to verify accuracy and completeness. Data from internal DOI systems is subjected to multiple automated checks for data completion and accuracy. Data from the DOI vendor, Skillsoft, concerning training course completion status and course progress tracking relies upon the vendor to verify accuracy and completeness. Individuals who complete courses receive confirmation and have the opportunity to contact the help desk to resolve any issues or incomplete or inaccurate information. Personnel data from Office of Personnel Management systems and payment confirmation data from Pay.gov relies upon the Office of Personnel Management and Department of the Treasury to verify accuracy and completeness. FedTalent maintains the data accuracy and completeness via custom rules that perform data validation routines prior to accepting information from external systems.

**B. How will data be checked for completeness?**

Employees and supervisors are responsible for ensuring data manually entered for training requests and performance appraisals is complete. Data from other systems is validated for completeness before it is imported into FedTalent. FedTalent maintains the data accuracy and completeness via custom rules that perform data validation routines prior to accepting information from external systems. The FedTalent system also utilizes application-level input validation with multiple data checks that inspects user input for expected results prior to accepting the information provided by the end user.

**C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).**

Personnel data is imported from the DOI FPPS on a daily basis to ensure the data is current. Payment data provided by users through Pay.gov for course payment is presumed to be current and accurate, and data verification processes are managed by the Department of the Treasury. eOPF data is updated by the Office of Personnel Management and this keeps the data current. WTTS and EODS data is updated regularly and this keeps the data current. Skillsoft training data is updated by the Vendor, and this keeps the data current.

**D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.**

DOI training records, except Ethics training (addressed below), are maintained under Department Records Schedule (DRS) - 1.2.0004, Short Term Human Resources Records (DAA-0048-2013-0001-0004), which was approved by the National Archives and Records Administration (NARA). The records disposition is temporary. The record will be cut off at the end of fiscal year in which files are closed. The records will be destroyed 3 years after cut-off.

Employee performance and competency management records are maintained under DRS 1.2.0005, Long Term Human Resources Records (DAA-0048-2013-0001-0005). The records disposition is temporary, and the records will be cut off at the end of the fiscal year in which the record is created. The contractor data will be cut off when the contractor separates or is no longer employed by the agency. Records must be retained 7 years after cut-off.

Federal agency customers are the owners of their own records and are responsible for identifying associated record retention schedules for their records and ensuring they are properly managed under the Federal Records Act.

Some agencies utilize NARA's General Records Schedule. Under this schedule, training records may be maintained under GRS 2.6, item 010 and 030, with a temporary retention of 3 years after superseded/obsolete. Non-SES performance records are also maintained under GRS 2.2, item 070, with a temporary retention of 4 years after date of appraisal. SES performance records may be maintained under GRS 2.7, item 072, with a temporary retention of 5 years after date of appraisal.

Ethics training certification is temporary, but maintained for 6 years, under GRS 2.6, item 020. This item is applicable to all Federal agencies and employees and is not superseded by the DRS.

**E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?**

Records are disposed of in accordance with the applicable records retention schedules for each bureau or office, Departmental policy and NARA guidelines. Paper records are shredded, and records contained on electronic media are degaussed or erased.

Federal agency customers are the owners of their own records and are responsible for the disposition of their records in accordance with the Federal Records Act.

**F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.**

There is a privacy risk to individuals in DOI FedTalent system due to the amount and nature of the data such as training and performance management information that may be received from DOI employees, volunteers, students and other DOI affiliates. The FedTalent system collects PII directly from the individuals. There is a privacy risk from the PII collected, processed and stored in FedTalent. These are mitigated through management, operational and technical controls that have been put into place to protect the confidentiality, integrity and availability of FedTalent system data.

FedTalent has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. FedTalent is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information. PII from FedTalent users is collected via encrypted internet connections. All internet connections with subscribing systems are NIST FIPS 140-2 compliant.

There is a risk that individuals may not have notice of the purposes for collecting their information, how it will be used, or that their PII is sourced from other DOI internal systems such as FPPS (Datamart) and shared with OPM. Individuals are notified of the privacy practices through published government-wide and DOI SORNs, Privacy Act Statements, Privacy Policy and Notices during the onboarding process, and user banners are posted on the client-facing website and applications. This PIA also provides a detailed description of DOI FedTalent system sources, data elements and how PII information is shared to help employees, contractors and other DOI affiliates to fully understand the system. Review of discrepancies relating to training and performance issues and responding to complaints would facilitate the efficient review and resolution of matters, to provide a factual basis for the improvement of DOI's policy.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. To mitigate this risk, access to files is strictly limited to

authorized personnel who require access to perform their official duties and specified as to the level of access within each bureau/office. In addition to physical controls, operational and technical controls in place to limit these risks include firewalls, encryption, malware identification, and periodic verification of system users. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels are enforced. The audit trail will include the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security.

There is a risk that DOI FedTalent may collect and share more information than necessary in conducting performance appraisals. To mitigate this risk, access to data is restricted and authorized personnel are instructed to be careful not to gather or store unnecessary information about individuals. There is a risk that data collected as part of the performance evaluation management process may not be accurate and may result in adverse performance decisions. HR personnel have the ability to update or make corrections to inaccurate HR data identified by an employee. Also, performance decisions are reviewed at multiple levels by designated reviewing officials.

There is a risk that information in the system will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored is limited to the minimal amount of data needed to meet Federal training and performance management requirements is maintained and used by the system. Records are maintained and disposed of in accordance with records retention schedules that were approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Documents pertaining to training and performance management in the FedTalent system are closely safeguarded in accordance with applicable laws, rules and policies.

DOI employees must take privacy, Federal Information Systems Security Awareness (FISSA), and records management training prior to being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

## Section 4. PIA Risk Review

**A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

☒ Yes: *Explanation*

FedTalent is a learning management and performance management system, and the use of personal data is both relevant and necessary to the use of the system.

☐ No

**B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?**

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

**C. Will the new data be placed in the individual's record?**

☐ Yes: *Explanation*
☒ No Not Applicable

**D. Can the system make determinations about individuals that would not be possible without the new data?**

☐ Yes: *Explanation*
☒ No

**E. How will the new data be verified for relevance and accuracy?**

Not applicable, new data is not being created.

**F. Are the data or the processes being consolidated?**

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

**G. Who will have access to data in the system or electronic collection? Indicate all that apply.**

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

FedTalent users can input and view their learning and performance information, but cannot access the information of others. Federal supervisory personnel are able to access the learning and performance information of their subordinates. DOI employees and support contractors access the system for management and daily operational purposes. External Federal customers access their own individual domain to manage their records in the system.

**H. How is user access to data determined? Will users have access to all data or will access be restricted?**

FedTalent users are only given access to data on a 'least privilege' basis. Employees will only have access to their personal learning and performance data. Supervisors will only have access to the learning and performance data of their respective subordinates. DOI employees and support contractors access the system for management and daily operational purposes based on least privileges necessary to perform their duties. External Federal customers have designated officials who are data custodians, and these officials determine appropriate access to their own records in the system.

**I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?**

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved with with the development and maintenance of the FedTalent System. Privacy Act contract clauses are included in the contract.

☐ No

**J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?**

☐ Yes. *Explanation*

☒ No

**K. Will this system provide the capability to identify, locate and monitor individuals?**

☒ Yes. *Explanation*

The FedTalent system is not intended to locate and monitor individuals. However, audit logs will capture required and relevant information concerning system users for the purpose of compliance with Federal cybersecurity regulations to protect the information system and data within the system. Audit logs capture information such as username, time and date of access, and other relevant user actions and activities.

☐ No

**L. What kinds of information are collected as a function of the monitoring of individuals?**

The FedTalent System Audit Logs collect information such as username, logon date and time, number of failed logon attempts, files accessed, and user actions or changes to records.

**M. What controls will be used to prevent unauthorized monitoring?**

The system will have the ability to audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. FedTalent System Administrators will review the use of FedTalent system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. FedTalent assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to FedTalent Rules of Behavior. Federal employees and Contractors must complete Federal Information System Security Awareness (FISSA) training, Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include username, logon date and time, number of failed logon attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

**N. How will the PII be secured?**

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training

☐ Other. *Describe*

**O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.**

The Associate Director, Human Resources Directorate (HRD), Interior Business Center serves as the DOI FedTalent Information System Owner and the official responsible for oversight and management of the DOI FedTalent security controls and the protection of customer agency information processed and stored by the DOI FedTalent system. The Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies. The Privacy Act system managers for the systems of records are responsible for ensuring the requirements of the Privacy Act are met for the learning management and performance management records maintained in the system, including the publication of a notice, decisions on Privacy Act requests, and responding to complaints, in consultation with DOI Privacy Officials. Federal agency customer data is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting requirements of the Privacy Act.

**P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?**

The DOI FedTalent Information System Owner and Information System Security Officer are responsible for oversight and management of the DOI FedTalent security and privacy controls, and for ensuring to the greatest possible extent that FedTalent is properly managed and that access is granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of data is reported to DOI-CIRC, and the customer agency if appropriate, within 1-hour of discovery in accordance with Federal policy and established DOI procedures.

External customer agency data is under the control of the customer agency. Each customer agency is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data in accordance with Federal policy and the terms of the service level agreement.