United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 12/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Talent Enterprise Diagnostic Tool (TED)	
Preparer: Michelle McClendon	**Office: OHR/PPTD/Workforce Planning Branch**
Date: 04/09/2020	**Phone: (202)564-3150**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☒ Implementation ☐	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐	
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).	

Provide a general description/overview and purpose of the system:

The EPA is establishing a new tool within the agency's existing SharePoint application. The tool is called the Talent Enterprise Diagnostic (TED) and provides for the collection of information to track, update, and assess the skills of positions throughout EPA along with the corresponding skills of incumbents in those positions. TED supports the agency's efforts to: 1) develop policies and programs that are based on comprehensive workforce planning and analysis; and 2) meet the requirements under 5 CFR 250, such as monitoring and addressing governmentwide and agency-specific skill gaps in mission-critical occupations. The system information will be accessed and used by employees' supervisors, designated human resources specialists and analysts, managers within each office and region, agency-wide senior leaders, and the agency's training branch.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

5 U.S.C. 1103 (Functions of the OPM Director, as it relates to identifying and closing competency gaps) and 5 U.S.C. 1402 (Authority and functions of agency Chief Human Capital Officers, as it applies to identifying and closing competency gaps.)

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

There is an existing System Security Plan for SharePoint, the application in which TED was created. Because SharePoint did not inherently have all the functionality needed, the Agency hired a consulting firm, CSRA/GDIT, to write new code within SharePoint to create TED. A separate System Security Plan was not completed for TED. TED is an application built within the Agency Sharepoint site all new code, is covered in the Workplace SORN and SSP.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

The data will not be stored in a Cloud.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

- Name of manager, supervisor, etc.
- Randomized SharePoint ID number
- Work Email
- First and Last Name of Employee
- Pay Plan

- Grade or Level
- Location
- Series
- Org Code
- Office/Region, Division, and Branch to which the position is assigned
- Occupational series/family
- Occupational specialty
- Name of skills and the proficiency level required for each position
- Name of skills and the proficiency level required for each incumbent in each position

2.2 What are the sources of the information and how is the information collected for the system?

The sources of information include data pulled from our personnel and payroll system (IBC/OBIEE) and supervisors' assessments of the skills proficiency levels required of each position under his/her immediate chain of command as well as assessments of the skills proficiency levels of each incumbent occupying those positions. The skills proficiency levels are selected from scale of numbers from 1 to 5, with 5 being the highest and 1 being the lowest.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The data within TED comes directly from our official payroll and personnel provider, IBC via its database (OBIEE). We rely on the accuracy of OBIEE data. Our Shared Service Centers enter data into our payroll and personnel system and we are relying on the controls instituted for that system. Any errors detected in TED will be promptly reported to the HRIT staff within the Office of Human Resources.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

1) **Privacy Risk:** EPA's Shared Service Centers enter data into our payroll and personnel system. They enter the data in accordance with OPM's standards and reporting requirements. We are relying on the controls instituted for that system. 2) There is a low

risk of human error leading to exposure of information during transmission process. WPB will provide the contractor with password-protected OBIEE data uploads to prevent PII risks.

Mitigation:

We will report errors detected in TED to the HRIT/OHR for correction. To reduce potential exposure of information during the transmission process, WPB will provide the contractor with password-protected OBIEE data uploads.

Section 3.0 Access and Data Retention by the system

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes. First, access to TED is only available through EPA's firewalls. That requires users to have access to SharePoint. Second, TED has access control levels to prevent authorized users from access to information they do not need to know. The three categories of users are Site Owners (Full Control) Site Members (Edit Access, which means that they can add, edit and delete lists; can view, add, update and delete list items and documents) and Site Visitors (Read Access, which means they can view pages and list items and download documents.). The Site Owners control who has access to TED- and at what level.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access control will be documented in TED SOP or/and TED user guide.

3.3 Are there other components with assigned roles and responsibilities within the system?

The contractor and staff within OHR/PPTD/Workforce Planning Branch have administrative access and are responsible for updating the system.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

No external parties, except contractors, will have access. Internally, supervisors, managers, HR

analysts and specialists, senior leaders, and administrators within TED will have access to data/information in the system. The contractor, CSRA/GDIT, has the Federal Acquisition Regulations (FAR) clauses included in its contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act).

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Information in TED and the data which is downloaded into Excel spreadsheets will be destroyed when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use. Information stored in TED falls under EPA's Records Control Schedule 1029 (Employee Training Program Records), Item a:

Item a: Employee training program records
https://intranet.epa.gov/records/schedule/final/1029.html

Includes: records about planning, assessing, managing, and evaluating EPA's training program including plans; reports and program evaluations; organizational and occupational needs assessments; employee skill assessments; employee training statistics; notices about training opportunities, schedules, or courses; mandatory training tracking and reporting files; logistics and coordination documents; Authorization, Agreement and Certification of Training (SF-182) and similar records; registration forms; employee attendance records; syllabi, presentations, instructor guides, handbooks, and lesson plans; reference and working files on course content; other course materials, such as presentations and videos; and student, class, or instructor evaluations.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

The risk related to retention is that the storage space on SharePoint reaches a limit or fails before three years.

Mitigation:

To compensate for the possibility of lost storage space, OHR will download and retain the data for the length of the retention schedule.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency

operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No – information will not be shared outside of EPA as part of the normal agency operations. Dummy data will be used in such circumstances.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

Information will not be shared outside of EPA as part of the normal agency operations. Dummy data will be used in such circumstances.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

NA

4.4 Does the agreement place limitations on re-dissemination?

NA

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

There is no privacy risk. Information will not be shared outside of EPA as part of the normal agency operations. Dummy and aggregated data will be used in such circumstances.

Mitigation:

None

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used in accordance with stated practices in this PIA (Section 6.1)?

There are user control levels coded into the system and the Agency will conduct periodic audits of reports generated, included who has accessed the system and when to ensure data is use for the purpose of collection.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The TED User guide will contain a link to the Privacy Act. Also, the agency requires all

employees to complete the annual Information Security and Privacy Awareness Training course.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

It is possible that the data could be altered in SharePoint or in the Excel spreadsheets.

Mitigation:

The system uses SharePoint's administrative control levels to determine who can see what within the overall system. As such, the administrators could see who would have made changes to the data- and when they were made. SharePoint has a feature that restores previous versions on documents to restore data integrity. Of course, once the data is downloaded and saved in Excel, the only mitigation is through a comparison between what is in SharePoint and what is in Excel. SharePoint also allows for an audit trail by tracking the activity/user actions of any item (document, event, task, etc.).

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

The system uses the position and incumbent skills assessments to create a competency gap analysis that identifies which skills are above and below the desired thresholds.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_ X No__. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

The primary retrieval method is employee name.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The main system, SharePoint, has an existing SORN. EPA-64.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Although TED is a management tool with restricted access, the data could be mistaken for use in decisions about individual employee performance.

Mitigation:

Throughout our briefings with management and potential users, we have emphasized that the TED is not used for individual employee performance. We will continue to discuss this in our briefings and add language to the TED homepage and in the user manual to remind users that the tool is not intended for use in individual employee performance. We use the SharePoint's version control feature to create an audit trail by tracking the activity/user actions of any item (document, event, task, etc.).

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

There are no opportunities for a non-supervisory employee to consent or decline to have their information in TED. TED requires certain employee data to carry out managerial and administrative obligations, such as workforce planning and training.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

There is a risk that individuals will not be aware that their information is collected and maintained in TED and that they may not understand how their information is being used.

Mitigation:

The risk cannot be mitigated through TED since TED does not collect information directly

from non-supervisory employees since they do not have access to the system. However, OPM's SORN OPM Govt -1 (https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf) informs employees of the human resources purposes for which their information is being collected. To the extent that the records listed here are also maintained in an agency electronic personnel or microform records system, those versions of these records are considered to be covered by this system notice. Any additional copies of these records (excluding performance ratings of record and conduct-related documents maintained by first line supervisors and managers covered by the OPM/GOVT-2 system) maintained by agencies at remote field/administrative offices from where the original records exist are considered part of this system.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

There is a risk that individuals will not be able to access and amend their information in TED.

Mitigation:

This risk is mitigated by the agency providing clear notice and instructions regarding access to and amendment of personnel records through the publication of OPM GOVT-1 SORN and this PIA.