United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(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: Technical Qualification Board (TQB)	
Preparer: Brodwynn Roberts	**Office: ORD/OARS/HRD**
Date: 7/2/2019	**Phone: 919-541-3894**
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 system automates the candidate application for promotions to the GS-14 or GS-15 grade levels for individuals engaged in research, development, or expert roles.

The system collects employee name, GS Level, ORD Organization, 1st line supervisor, 2nd line supervisor, current grade, ORD organization, TQB Coordinator (employee), ORD Rep (employee), TQB Chair, Program/Region Representative (employee), TQB Peer (employee), 2 Peer Reviewers (ad-hoc panel members, nonFED) [name, the following information may be business or private due to possibility of ad-hoc being working or retired: mailing address, eMail, phone number, Title, Specialty, and their organizational name). Employee also uploads files; cannot enforce what they upload.

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?

In accordance with ORD Policy, the NHEERL Technical Qualifications Board (TQB) reviews the credentials of employees in research, expert, and development positions who are recommended for promotion to the GS-14 and 15 grade levels.

5 U.S.C., Part III - Employees, Subpart D – Pay, Allowances

5 CFR

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?

Salesforce platform authorized by OSM/OEI for agency use. Not accessible without an EPA email address. Salesforce has its own security plan which our system falls under.

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. The was a paper process leaned by the ORD Management Council approval.

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?

Data will be stored in the Salesforce EPA cloud. The Salesforce cloud has an ATO.

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).

Names, work addresses, work telephone numbers, work emails of employees.

For Non-government contributors and external Peer Reviewers data may be their employer or personal as they provide us: Names, addresses, telephone numbers, and emails.

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

EPA candidate enters this information required in the TQB application.

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

No.

2.4 Discuss how accuracy of the data is ensured.

Data is provided and authenticated by the candidate, verified by 1st and 2nd line supervisors, and the TQB Coordinator.

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.

Privacy Risk:

None. It is shared with known external Peer Reviewers, accepted by candidates who know their data is being shared. Candidate is aware data is being shared with external Peer Reviewers.

Mitigation:

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, there are four levels of access as described below:

TQB Candidate can only see his data.

TQB Chair can only see packages assigned to him/her

1st and 2nd line supervisors can only view their branch/division's information

TQB Coordinator can see all applications/packages

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

The Salesforce admins provide different level of access based on guidance from the TQB Coordinators.

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

No.

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 contractors will have access to the system.

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.

Records retention is for 5 years, and we store the data in one place and purge the data after 5 years when action is completed. Data will be purged every 5 years according to EPA Records Schedule 0572

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:

None. Records retention is for 5 years, and we store the data in one place and purge the data after 5 years when action is completed. Data will be purged every 5 years according to EPA Records Schedule 0572

Mitigation:

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.

Yes, the candidate package is either emailed or printed sent United Parcel Service (UPS) to external Peer Reviewers.

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

External Peer Reviewers must review package and provide feedback. There is no access to system for them. External Peer Reviewers are told to destroy package after their review as per their contract.

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?

N/A

4.4 Does the agreement place limitations on re-dissemination?

Once the data is sent to the external Peer Reviewers, the external Peer Reviewers do not share with anyone else.

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:

No risk since the information is not shared with external parties.

Mitigation: n/a

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)?

ORD supervisors (1st and 2nd line), TQB Coordinator, will approve Candidate's package to move forward. TQB Chair coordinates with all reviewers, both internal to EPA and external to EPA, to receive feedback. (The Candidate Package review information is discussed with agency Panel Members and outside panel members, outside of system, determine eligibility.) Then TQB Chair or TQB Coordinator updates the system. This is based on access control levels.

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

Nothing other than the annually required EPA training. First time users are also trained on TQB system.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

None. Auditing and accountability controls are inherited by the Salesforce Cloud.

Mitigation:

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 Candidate inputs / uploads their package into the system to apply for a promotion. The package is then reviewed by peer reviewers to determine eligibility. The system collects the data and tracks the status of the process.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X__. 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.*)

It is retrieved by a computer generated number.

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

None

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:

None, only internal users have role-based uses and access to the data in the system.

Mitigation:

*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.

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?

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:

Mitigation:

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?

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

8.3 How does the system notify individuals about the procedures for correcting their information?

8.4 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:

Mitigation: