United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. ***All entries must be Times New Roman, 12pt, and start on the next line.*** If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Ethnicity, Race and Gender Information	**System Owner: Robersena Young-Mackall**
Preparer: Gina Moore	**Office: OMS-OIE-FACMOD**
Date: August 23, 2024	**Phone: 202-564-0462**
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 Ethnicity, Race and Gender Identification form was developed in compliance with Executive Order 14035, Section 5(e) for federal advisory to collect voluntarily self-reported demographic data to be displayed on a diversity dashboard as a snapshot of the Agency's federal advisory committees. The information collected will only be used as aggregate data displayed on a diversity dashboard. The forms will be stored in a secure EPA OneDrive/Sharepoint folder with very limited access, without any personal identifiers within the file name. Once the aggregate data has been collected from the original form and, the form will not be reviewed/revisited for additional analysis. The original forms will be kept for up to three years, based on membership terms. No document will be kept over six years (two terms maximum per member).

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?

President Biden's Executive Order (EO) 14035, on *Diversity, Equity, Inclusion, and Accessibility* (DEIA) in the Federal Workforce, of June 25, 2021, Section 5(e), Data Collection

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?

The program is utilizing OneDrive/Sharepoint to store the forms relying on the M365 ATO. The program itself will not be issued an ATO.

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.

The Ethnicity, Race and Gender Identification Form was assigned OMB Control NO. 2030-0055, Approval Expires 07/31/2027.

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?

Yes, utilizing OneDrive/Sharepoint to store the forms.

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).

The form collects the following demographic data from federal advisory committee nominees: name, gender, ethnicity, sexual orientation, and accessibility. Nominees are not federal government employees, rather members of the public.

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

When EPA solicit nominations via a federal register notice for federal advisory committee members, nominees will be asked to submit the form to self-report ethnicity, race, gender and accessibility similar to resumes, CVs, bios.

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, in-house form

2.4 Discuss how accuracy of the data is ensured.

Applicants will voluntarily complete information on the form and the information is as accurate as the applicant completing the form discloses.

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:

There is a risk that false data will be submitted.

Mitigation:

The information is as accurate as what the submitter provides. This is information optional and will only be used in aggregate, statical reporting as instructed in E.O. 14035.

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?

On OneDrive, the Federal Advisory Committee Management and Oversight Division (FACMOD) staff will be the keeper of the original files and will have administrative control access in addition to adhering to EPA cybersecurity and privacy training policies access to these files are limited and controlled.

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

Access to information is controlled through Active Directory (AD) via Access Control List (ACL). Access can be revoked or edited by the site owner using the ACLs. The Federal Advisory Committee Management and Oversight Division Director determines the roles and what information can be accessed by which user on the staff.

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

There are no other components with assigned roles and responsibilities on the Ethnicity, Race, and Gender Identification Form. Nominees voluntarily self-identify demographic data. No other components will have access to this data.

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?

Contractors will not have access to the data. Government employees have access to the data/information in the Ethnicity, Race and Gender Identification Form. Only personnel (designated EPA full time employee) with system administrator accounts can access the data. All users must be approved and must have proper authentication credentials to be able to access the data on the form.

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.

The form is considered a non-substantive committee record under EPA Records Schedule 1024: Federal Advisory Committee Records, Item e and is disposable after three years.

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

There is a risk that these files will be held at EPA indefinitely.

Mitigation:

Per EPA Records Schedule 1024e, the forms will be destroyed after three years.

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.

There is no external sharing.

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

No, the form doesn't share information outside of EPA.

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?

N/A

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:

NA. There is no external sharing.

Mitigation:

NA

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 as stated in Section 6.1?

EPA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of the information.

5.2 Describe what privacy training is provided to users either generally or

specifically relevant to the system/collection.

The EPA implements cybersecurity Rules of Behavior (ROB) for which all users must consent prior to being granted credentials for access. In addition, all EPA personnel receive annual refresher Information Security Privacy Awareness Training (ISPAT) to educate them regarding the use and management of sensitive data along with other mandatory training tracked in FedTalent.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a risk that someone at EPA will have unauthorized access to these demographic files.

Mitigation:

FACMOD staff will be the keeper of the original files and will have administrative control access in addition to adhering to EPA cybersecurity and privacy training policies. Access to these files is limited and controlled.

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.

When EPA solicit nominations via a federal register notice for federal advisory committee members, nominees will be asked to submit the form to self-report ethnicity, race, gender and accessibility similar to resumes, CVs, bios.

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.)

The form will be kept in the corresponding committee membership folder on a folder on One Drive in the Federal Advisory Committee Management and Oversight Division. The forms will not be searchable or retrievable by name or other identifying means. The naming convention tentatively will be the abbreviation of the committee, followed by member and a number. A staff member will have to go into the membership committee folder and would have to open the document to see the name of the person that completed it. This is to ensure maximum privacy. See example below:

For someone on the Board of Scientific Counselors (BOSC), their form would be stored in the folder as follows:

- BOSCMember1

- BOSCMember2
- And so on

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

All access is maintained by EPA. There are administrative and technical controls in place to protect information, such as access control lists, PIV cards and passwords. These are tested annually.

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:

The demographics data can be misused for other reasons than its intended purpose of providing voluntary statistical data for reporting purposes

Mitigation:

The EPA implements a Rules of Behavior (ROB) for which all users must consent prior to being granted credentials for access. In addition, all EPA personnel receive annual refresher Information Security Privacy Awareness Training (ISPAT) to educate them regarding the use and management of sensitive data. Finally, this secure folder is only accessible by one designated EPA employee who follows EPA cybersecurity procedures and policies.

***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

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 Privacy Impact Analysis: Related to Redress

Privacy Risk:

Mitigation: