

Office of Government Ethics

Professional Ethics Practitioner Certificate Program (PEP) Reporting Application Privacy Impact Assessment

November 2023
Program Counsel Division

**U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for PEP Reporting Application**

Provide electronic copies of the signed PIA to OGE’s Chief Information & Cybersecurity Officer and Privacy Officer.

Name of Project/System: Professional Ethics Practitioner Certificate Program (PEP) Reporting Application Privacy Impact Assessment

Office: Program Counsel Division

Executive Summary

It is intended that this PIA will cover the collection of data necessary to provide certification for federal ethics officials completing the requirement to satisfy the annual PEP requirement. This information will also be helpful to OGE in evaluating the attendance and interest in the courses offered throughout the calendar year. The proposed application will be hosted on OGE’s website and developed by staff. Information will be stored within the application and not downloaded to OGE’s network. The application will contain historical information for a one year period and a new application built each year. This PIA covers subsequent applications as long as the functionality is identical to the original. If the functionality is modified, a PTA must be submitted and a modification to this PIA may be required.

A. CONTACT INFORMATION:

1) Who is the person completing this document

Anna Wheeler
Senior Instructor
Institute for Ethics in Government
Program Counsel Division
awheeler@oge.gov
202-482-9285

2) Who is the system owner:

Nicole Stein
Chief, Agency Assistance Branch
Program Counsel Division
nstein@oge.gov
202-482-9255

3) Who is the system manager for this system or application:

Anna Wheeler

Senior Instructor
Institute for Ethics in Government
Program Counsel Division
awheeler@oge.gov
202-482-9285

4) Who is the Chief Information Security Officer (CISO) who reviewed this document?

Ty Cooper
Chief Information & Cybersecurity Officer
Information Technology Division
jtcooper@oge.gov
(202) 482-9226

5) Who is the Senior Agency Official for Privacy who reviewed this document?

Diana J. Veilleux
Senior Agency Official for Privacy and
Chief, Legal, External Affairs and Performance Branch
Program Counsel Division
Diana.veilleux@oge.gov
202-482-9203

6) Who is the Reviewing Official?

Ty Cooper
Chief Information & Cybersecurity Officer
Information Technology Division
jtcooper@oge.gov
202-482-9226

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. Applications submitted through this form will contain information about individuals who are executive branch employees. It will include their names, government e-mail address, employing agency, how long they have been performing ethics duties, the average number of hours they spend on ethics, whether they identify as a member of an underserved community, why they participated in the PEP program, and OGE IEG courses taken throughout the calendar year.

a. Is this information identifiable to the individual?

Yes.

b. Is the information about individual members of the public?

No, application will be limited to current federal employees.

c. Is the information about employees?

Yes.

2) What is the purpose of the system/application?

The application will allow users to self-report their attendance of PEP courses throughout the year to receive a certificate. This information will also be used by OGE to evaluate the effectiveness of the courses.

3) What legal authority authorizes the purchase or development of this system/application?

The PEP program is conducted under OGE's organic authority to provide the executive branch with information about ethics law and policy. See 5 U.S.C. § 13122(b)(14).

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Current executive branch employees, potentially including OGE employees.

2) What are the sources of the information in the system?

Information is collected from the applicants themselves.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

See above.

b. What federal agencies provide data for use in the system?

Individuals from potentially any executive branch agency may provide data as well individuals from ethics offices within the legislative or judicial branches.

c. What State and local agencies are providing data for use in the system?

None.

- d. From what other third party sources will data be collected?**

N/A.

- e. What information will be collected from the employee and the public?**

See section B.1.

3) Accuracy, Timeliness, Reliability, and Completeness

- a. How will data collected from sources other than OGE records be verified for accuracy?**

Applicants are responsible for providing accurate information.

- b. How will data be checked for completeness?**

The application will use validation to ensure complete responses are submitted. More specifically, the application will provide an error message if an individual does not complete all of the required fields. In addition, there is an attestation statement on the form: "By clicking the button below, 'Submit', I attest that all information reported above is accurate and complete."

- c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?**

Not applicable. The data is intended to be current when collected and then will be used for historical purposes only. A new application will be built each year.

- d. Are the data elements described in detail and documented?**

No. However, the data elements are simple and self-explanatory.

D. ATTRIBUTES OF THE DATA:

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

3) Will the new data be placed in the individual's record?

N/A.

4) Can the system make determinations about employees/the public that would not be possible without the new data?

N/A.

5) How will the new data be verified for relevance and accuracy?

N/A.

6) If the data is being aggregated, what controls are in place to protect the data from unauthorized access or use?

Although the data will be aggregated, the aggregated data is anonymized from individual identification. See below for controls in place to prevent unauthorized access.

7) How will the data be retrieved? Does a personal identifier retrieve the data?

Self-reported attendance will be retrieved by personal identifier, typically applicant's name.

8) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The reports will be used to assess the utility of the program, as well as for agency performance documents. Anyone who has been authorized to use the application using the AARF process will have access to the reports in the application.

Reports to be produced will include:

- Number of individuals that earned a certificate from underserved communities
- Number of individuals that earned a certificate by the amount of experience they have as well as the amount of time they spend on ethics
- Number of individuals that earned a certificate
- Number of agencies who had individuals earn a certificate
- Number of people who took individual IEG PEP offerings

9) What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)?

Participation in the PEP certificate program is entirely voluntary. All requested information must be provided for an applicant to receive their certificate. There is no opportunity to consent to particular uses of the information. A Privacy Act statement will be included on the application.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Not applicable.

2) Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?

The records are covered by General Records Schedule 2.6, Item 030. The records are to be destroyed when superseded, three years old, or one year after separation, whichever comes first, but longer retention is authorized if required for business use.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Timely destruction of federal records is the responsibility of the agency Records Officer. The reports are temporary and will be destroyed in accordance with OGE NARA-approved records disposition schedules.

4) Is the system using technologies in ways that the OGE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

OGE has designed the application form to collect only that information necessary to confirm that certificate requirements have been met.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

7) What kinds of information are collected as a function of the monitoring of individuals?

N/A.

8) What controls will be used to prevent unauthorized monitoring?

N/A.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

The PEP certificate program is collected and maintained pursuant to OGE/INT-6, Registration and Administration Records for OGE-Hosted Meetings, Events, Educational and Training Programs, and Professional Development Offerings. The application will display a Privacy Act statement.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

No.

F. ACCESS TO DATA:

1) Who will have access to the data in the system?

Only a limited number of OGE users will have direct administrative access to the application and to the information collected through the application. Only authorized OGE users will have access to the data that is imported into OGE's network through the application. Generally, the information collected will be limited to non-sensitive PII, such as name, e-mail address, and agency.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to OGE applications and user accounts is governed by the Account Access Request Form (AARF) process, which authorizes the Information Technology Division (ITD) to create, modify, and disable network accounts, including providing access to OGE applications. AARF requests must be signed by the employee, his/her supervisor, and the Chief Information & Cybersecurity Officer before a request is approved to be implemented by ITD staff.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Users will only have access to the data they are authorized to access.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

Because administrative access is restricted to a very limited number of authorized individuals, there is no potential for unauthorized browsing.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

No.

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

No.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

N/A.

- 8) Will other agencies share data or have access to the data in this system (Federal, State, or Local)?**

No.

- 9) How will the data be used by the other agency?**

N/A.

- 10) Who is responsible for assuring proper use of the data?**

Each authorized user is responsible for assuring proper use of the data collected.

See Attached Approval Page

The Following Officials Have Approved the PIA for PEP Reporting Application:

1) System Manager/Owner

Electronic
Signature: nes

Name: Nicole Stein
Title: Chief, Agency Assistance Branch

2) Chief Information & Cybersecurity Officer

Electronic
Signature: TC

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer

3) Senior Agency Official for Privacy

Electronic
Signature: DJV

Name: Diana Veilleux
Title: Chief, Legal, External Affairs and Performance Branch and Senior Agency Official
for Privacy