Office of Government Ethics

Privacy Impact Assessment for the Confidential File Room

February 2021

General Counsel and Legal Policy Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for the
Confidential File Room

Provide electronic copies of the signed PIA to OGE's Chief Information Security Officer and Privacy Officer.

Name of Project/System: Confidential File Room
Office: General Counsel and Legal Policy Division

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Jennifer Matis
Privacy Officer
jmatis@oge.gov
202-482-9216

2) Who is the system owner?

David J. Apol
General Counsel
djapol@oge.gov
202-482-9205

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

Deborah J. Bortot
Chief
Presidential Nominations Branch
djbortot@oge.gov
202-482-9227

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

Ty Cooper
Chief Information Officer
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
Chief, Legal, External Affairs and Performance Branch
Diana.veilleux@oge.gov
(202) 482-9203

6) Who is the Reviewing Official?

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

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. The application contains Confidential Financial Disclosure Reports (OGE Form 278C and OGE Form 450) and Ethics Agreements for nominees confirmed by the U.S. Senate, and individuals who were considered but not confirmed by the U.S. Senate or withdrew from consideration for the position. It also contains source documents (e.g., emails, notes, background research reports, etc.) used to memorialize comments of filers in response to review questions, and other supporting documentation.

a. Is this information identifiable to the individual?

Yes.

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

Yes, it includes information about nominees to Senate-confirmed Presidential appointee (PAS) positions.

c. Is the information about employees?

Yes, it includes information about federal appointees who may or may not be an employee.

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

The purpose of the application is to create a secure electronic filing repository for confidential nominee financial disclosure reports and related records that are reviewed or created by OGE as part of the confirmation process.

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

The Ethics in Government Act of 1978, as amended, and OGE's regulation at 5 CFR part 2634 govern the filing of financial disclosure reports, as well as OGE's role in that process. The Ethics in Government Act of 1978 also authorizes the Director of OGE to provide overall direction of executive branch policies related to preventing conflicts of interest on the part of officers and employees of any executive agency. See 5 U.S.C. app. § 402(a).

C. DATA in the SYSTEM:

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

Nominees to be confirmed by the U.S. Senate and individuals who were considered but not confirmed by the U.S. Senate or withdrew from consideration for the position.

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

Most of the personally identifiable information (PII) in the system is provided by the individuals on their financial disclosure report (OGE Form 450 or confidential 278) and/or draft ethics agreement. OGE staff add supporting documents concerning the review process.

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?

As described above, the PII in the system is obtained directly from the individual. The information may be forwarded through the designated agency ethics official (DAEO) of the executive branch agency to which the individual has been nominated or appointed. Similarly, there are also nominees at nongovernmental agencies, and information on those nominees may be provided through the nongovernmental employing organization. However, in all cases the information originates with the individual.

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

As described above, information may be provided by the DAEO of any executive branch agency.

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?

None.

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

As described above, information is collected from employees and the public on their financial disclosure report and/or draft ethics agreement, including information on financial assets, financial transactions, and current and former positions held.

3) Accuracy, Timeliness, Reliability, and Completeness

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

Individuals are responsible for the accuracy of the information they provide to OGE directly or indirectly through their DAEO.

b. How will data be checked for completeness?

OGE staff will check the data for completeness as part of OGE's business process.

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

OGE staff ensure that the data is kept current based on information reported to OGE from the individual. Once the confirmation process is complete, the information is purely historical and is not intended to be kept current.

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

The application is primarily a document filing system and contains only the data elements necessary for document and records management purposes.

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?**

Access to the system is limited to authorized users. Authorized users have been advised that agency policy prohibits them from unauthorized use of data and have been instructed not to engage in such activities.

7) **If data is being aggregated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

Yes, see above.

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

Data is retrieved by personal identifier.

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

The application cannot produce reports.

10) 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)?

Providing the information is required of all nominees. Individuals do not have any opportunity to consent to particular uses of the information.

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?

N/A.

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?

Yes, they are covered by General Records Schedule 2.8.

Nominee confidential financial disclosure reports (for nominees not subsequently confirmed by the Senate) are destroyed one year after the nominee ceases to be under consideration for the position. All other confidential financial disclosure reports are destroyed six years after receipt by the agency. Financial disclosure supporting documentation is destroyed at the same time an individual's related financial disclosure report is destroyed or 6 years after the individual has submitted their last financial disclosure report. In all cases, the records can be preserved while needed for an active investigation. Otherwise, the disposition instruction is mandatory and longer retention is not allowed.

Related records for employees who file financial disclosure reports are destroyed at the same time as the employee's last related financial report or when no longer needed for active investigation, whichever is later. Longer retention is authorized if needed 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?

Approved disposition methods for the disposition of the data at the end of the retention period include shredding for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines. Procedures for the disposition of OGE data is included in OGE's managing electronic records guidance and policy documentation, as well as the OGE Network System Security Plan.

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?

The application will be more secure than the current hardcopy file room used to store these records. Therefore it will enhance public/employee privacy.

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.

OGE/GOVT-2, Executive Branch Confidential Financial Disclosure Reports.

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

The system of records notice will not require amendment or revision. The application is merely creating an electronic records room for records now kept in hardcopy.

F. ACCESS TO DATA:

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

Authorized OGE employees have access to the data in the application.

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

Access to OGE applications 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 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.

Authorized users will have access to all data in the system.

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

Authorized users have been advised that agency policy prohibits them from unauthorized browsing of data and have been instructed not to engage in such activities.

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 contractors were involved with the design, development, or maintenance of the system.

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.

See Attached Approval Page

The Following Officials Have Approved the
PIA for the Confidential File Room:

1) System Manager

Initials: DJB Date: 1/22/2021

Name: Deborah J. Bortot
Title: Chief, Presidential Nominations Branch

2) System Owner

Initials: DJA Date: 2/1/2021

Name: David J. Apol
Title: General Counsel

3) Chief Information Officer

Initials: TC Date: 12/29/20

Name: Ty Cooper
Title: Chief Information Officer

4) Senior Agency Official for Privacy

Initials: DJV Date: 12/16/20

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