Office of Government Ethics

Legal Expense Fund Management System
Privacy Impact Assessment

March 2024

General Counsel Law and Policy Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for the
Legal Expense Fund Management System

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

Name of Project/System: Legal Expense Fund Management System
Office: General Counsel and Legal Policy Division (GCLPD)

Executive Summary

OGE published a Final Rule creating a new subpart J to the Standards of Conduct, governing the establishment of legal expense funds for government employees. This regulation requires employee beneficiaries to submit trust documents and quarterly reports to agency ethics officials and, in certain cases, to OGE for review. In addition, all trust documents and quarterly reports (other than those filed by anonymous whistleblowers or those that contain classified information) will be posted by OGE to the OGE website. GCLPD worked with the Information Technology Division (ITD) to create a new web application to serve as the Legal Expense Fund Management System for the trust documents and quarterly reports. This PIA covers both OGE's program implementing the regulation and the application.

In addition to the Legal Expense Fund Management System application, information collected and maintained as part of this program may also be stored temporarily on OGE "HOME" network drives (including the "downloads" folder). It will not be placed on unrestricted network drives. Finally, a separate, more secure application will be developed to house anonymous whistleblower records collected and maintained as part of this program and whistleblower documents will be transmitted to OGE through a dedicated Outlook email address. A separate PIA will be created for the whistleblower application and the related processes.

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Maura Leary
Associate Counsel
Ethics Law and Policy Branch
General Counsel and Legal Policy Division
mleary@oge.gov
202-482-9231

2) Who is the system owner?

David Apol
General Counsel
General Counsel and Legal Policy Division

djapol@oge.gov
202-482-9205

3) Who is the system manager?

Maura Leary
Associate Counsel
Ethics Law and Policy Branch
General Counsel and Legal Policy Division
mleary@oge.gov
202-482-9231

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

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

6) Who is the Reviewing Official?

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

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. This system includes the name, position, and employing agency of employee beneficiaries. The system also includes the names and contact information of trustees/representatives; the name, city and state, employer, and donation amount of donors; the name and payment amount of payees; the name and official government phone number and email address of the agency contact; and the name of the OGE reviewer. Note that although the regulation provides for special protection for

beneficiaries who are anonymous whistleblowers, this application will not contain any records from such anonymous whistleblowers.

a. Is this information identifiable to the individual?

Yes.

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

Yes. Some information is about individual members of the public– specifically, the names, city/state, and employers of donors, the names of and contact information for trustees/representatives, and the names of payees.

c. Is the information about employees?

Yes. Some information is about employee beneficiaries– specifically, the employee's name, position, and agency. The system also contains the agency contact's name and official government phone number and email address as well as the name of the OGE employee reviewer.

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

The purposes of the program and related application are: (1) to track all legal expense funds established/terminated in accordance with subpart J; (2) to facilitate review of certain legal expense trust fund documents and quarterly reports by OGE employees in accordance with subpart J; and (3) to post to OGE's website all legal expense trust fund documents and quarterly reports, including termination reports, other than those that have been specifically exempted (those of anonymous whistleblowers and those containing classified information).

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

Title IV of the Ethics in Government Act of 1978; sections 201(a) and 403 of Executive Order 12674 (as modified by E.O. 12731); 5 U.S.C. §§ 7301, 7351(c), and 7353(b)(1); 5 CFR part 2635, subpart J.

C. DATA in the SYSTEM:

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

This system contains records about executive branch employees who seek to create a legal expense fund, pursuant to 5 CFR part 2635, subpart J, for the purpose of accepting donations and disbursing payments for legal expenses for a matter arising in connection

with the employee's past or current official position, the employee's prior position on a campaign, or the employee's prior position on a Presidential Transition Team. Information may be collected or remain in the system after the employee beneficiary has left employment with the executive branch. This system also contains records about executive branch employees who serve as the agency contact for a legal expense fund and OGE employees that are assigned to review legal expense fund documentation. This system also contains records about members of the public who contribute payments for legal expenses (donors), members of the public who receive payments for legal expenses (payees) and members of the public who serve as a beneficiary's trustee or representative in establishing and maintaining a legal expense fund.

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

The information is collected from the legal expense trust fund documents and the quarterly and termination reports. These documents will be filled out by either the employee beneficiary or the trustee and emailed to a program-specific email address. OGE staff will review the email inbox, upload the documents to the application, and enter additional data into the application, such as date received.

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?

The information is collected directly from the individual by the employee beneficiary or their trustee/representative.

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

Any executive branch Federal agency may provide information for use in the system.

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?

Reviewers may add to the system notes based on information from third party sources about entities cited in reports. Such third party information will be collected only from publicly available internet sources (i.e. googling). No other data will be collected from third party sources.

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

- For employee beneficiaries: their name, position, and agency.

- For employee agency contacts: their name, phone number, and email address.
- For OGE employee reviewers: their name.
- For trustees/representatives: their name and contact information.
- For donors: their name, city and state, employer, and amount donated.
- For payees: their name and amount received.

3) Accuracy, Timeliness, Reliability, and Completeness

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

OGE will rely on the employee beneficiaries and trustees to provide their own information accurately through the legal expense trust fund documents and the quarterly and termination reports.

b. How will data be checked for completeness?

Agency ethics officials and OGE will review documents to be posted for completeness and return to the employee beneficiary if additional data is needed.

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

Most of the information is intended to be historical and not continuously updated. The information that is appropriately maintained as current, such as trustee contact information, will be updated from quarterly reports and ongoing contact with the individuals providing information.

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

The following data elements are listed in the quarterly/termination report form and in the draft trust guidance:

- For employee beneficiaries: their name, position, and agency.
- For employee agency contacts: their name, phone number, and email address.
- For OGE employee reviewers: their name.
- For trustees and representatives: their name and contact information.
- For donors: their name, city and state, employer, and amount donated.
- For payees: their name and amount received.

The other data elements contained in the application are not documented but 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?

The program collects, maintains, and–in part–releases information not previously collected by the executive branch. Much of that information will be stored in the application and eventually made public per the requirements of the regulation. Although the information may be aggregated when made public, this application does not have the capability to aggregate information about individuals.

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

The application maintains individual records for each employee beneficiary. However, these records are not linked to any other records on that individual, such as records regarding their financial disclosures.

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

The system cannot; however, individuals who review the data can determine who is donating to a specific employee's legal expense fund and to whom the employee is paying out of the fund for legal services.

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

OGE will rely on the employee beneficiary and trustee to provide accurate information.

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

Not applicable; the system is not capable of aggregating information on individuals. Although there is a potential for aggregation once the information is made public, that transparency is an essential element of the policy and by definition is not unauthorized.

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

Not applicable.

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

The application and the external application that posts the documents on oge.gov both contain a searchable database. It is possible to search by the employee's name, position, and agency, date OGE received the document, and the type of document. It is also possible to search by the name of the OGE employee reviewer. It is not searchable by any other 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?**

No reports are produced on individuals.

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)?**

Individuals may submit reports anonymously if they believe themselves to be a whistleblower as defined by the regulation. Apart from this option, if an employee beneficiary wishes to establish an LEF, or if an individual wishes to serve as a trustee of, donate to, or receive payments from an LEF, providing this information is required rather than voluntary. They cannot 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?**

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?**

OGE records dispositions are pending. Related records will be maintained as permanent as required by the National Archives and Records Administration (NARA) until NARA has approved the retention and disposition schedule related to records for proposed 5 CFR part 2635, subpart J.

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?**

See above. Until a records disposition authority is approved, the records will be maintained permanently.

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 program and related application have a moderate effect on privacy for employee beneficiaries, trustees, representatives, donors, and payees. This is information that was not previously collected by the executive branch. However, most of the information in the system does not carry a significant risk for the individuals affected. Much of it, in fact, is legally required to be made public.

The impact on privacy has been minimized in the following ways. The regulation was drafted to minimize the amount of personally identifiable information (PII) collected and released to only that necessary to meet the purposes of the policy, and employee beneficiaries will be asked to avoid including any unnecessary PII when they submit legal expense fund documents. Beyond this required information, the application will contain only non-sensitive PII required to administer the program, such as OGE employee assignments. We have standard operating procedures (SOPs) in place to ensure that unnecessary PII is not placed in the system or released online. The SOP includes instructions that individuals should not include unnecessary PII in their trust documents or reports, as well as instructions to ethics officials and OGE staff to review the documents to check whether such PII has been inadvertently included.

The following controls are in place to ensure that sensitive PII is not inadvertently released on OGE's website:

- If OGE discovers that unnecessary PII has been submitted, the employee beneficiary (or their trustee/representatives) will be asked whether they want to have the original version published to the website or to have the unnecessary PII removed before posting. If a revised version is created, the original version will be removed from the system.

- OGE employee reviewers, as part of their standard operating procedures, will review all documents prior to posting on the website. Documents will not be posted to the website until the OGE employee reviewer marks the report as ready to be posted.

- As stated below, there is no integration in place to automatically post documents to the website. After the OGE employee reviewer indicates a

document is ready to be posted, the document must be removed from the application and manually posted to the website by a member of ITD.

All employee beneficiaries, as well as potential trustees, representatives, donors, and payees, are notified about the use of the data and public posting requirements; they also are provided a Privacy Act statement.

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?

Not applicable.

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

The system does not have the capability to monitor individuals.

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

A new system of records, OGE/GOVT-3, Legal Expense Fund Trust Documents, Reports, and Other Name-Retrieved Records, has been created for the information maintained in this system.

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

Not applicable, the system is new.

F. ACCESS TO DATA:

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

ITD has strict controls over the application database; only ITD developers and the LEF program managers and their supervisors have access to the data.

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

Only OGE employees required to review LEF trust documents or quarterly report information as part of administering the LEF regulation will be granted access to the application and the program-specific email account. 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 & 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 are able to view all data. However, only the program manager will be able to edit all fields.

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

Users cannot access records that they are not authorized to access, thus preventing unauthorized browsing. In addition, 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.

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

Some of initial data in this system (e.g., list of agencies) was initially pulled from another OGE application, the Financial Disclosure Tracking System (FDTS). However, the two systems are now decoupled. There is no integration sharing data out of the system into another system.

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

Not applicable.

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?

Not applicable.

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

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

The Following Officials Have Approved the PIA for Vulnerability Disclosure Policy:

1) **System Manager**

   Electronic
   Signature:

   Name: Maura Leary
   Title: Associate Counsel, Ethics Law and Policy Branch

2) **System Owner**

   Electronic
   Signature:

   Name: David Apol
   Title: General Counsel, General Counsel Law and Policy Division

3) **Chief Information & Cybersecurity Officer**

   Electronic
   Signature:

   Name: Ty Cooper
   Title: Chief Information & Cybersecurity Officer

4) **Senior Agency Official for Privacy**

   Electronic
   Signature:

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