OGE eForm 450 Phase 2 Project (eForm450)

Privacy Impact Assessment (PIA)

September 24, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Nathaniel Ciano

Name of Program Manager/System Owner:

- Linda Espejo

Signature Page

Signed:

DocuSigned by:
Nathaniel Ciano
113E72276281433...
Information System Security Manager (ISSM)

DocuSigned by:
Linda Espejo
F53F7FFEF56A455...
Program Manager/System Owner

DocuSigned by:
Richard Speidel
171B5411183F40A...
Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
06/08/2020	Initial Draft of OGE eForm 450 Project PIA Update	1.0
9/21/2020	Updated ISSM and document formatting	2.0
9/24/2020	Addressed Privacy Officer's Comments	3.0

Table of contents

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about OGE eForm 450 Phase 2 Project (eForm450). To accomplish its mission, *GSA* OGE (Office of Government Ethics) must, in the course of Ethics Program, collect personally identifiable information (PII) about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

A. System, Application, or Project Name:

OGE eForm 450 Phase 2 Project (eForm450) is under Enterprise Application Services (EAS) of FISMA System.

https://www.gsa.gov/cdnstatic/EAS_PIA_August2020.pdf

B. System, application, or project includes information about:

Confidential Financial Disclosure Report to avoid involvement in a real or apparent conflict of Interest of GSA employees in certain positions as determined by the GSA OGE.

C. For the categories listed above, how many records are there for each?

Near 7,000 records each year starting from 2021.

D. System, application, or project includes these data elements:

- *Employee Name*
- *Employee agency, branch, grade, position, outside positions*
- *Contact information (e.g., address, telephone number, email address);*
- *Financial Information (assets and income, liabilities);*
- *Agreements and Arrangements*
- *Gifts and Travel Reimbursements*

Overview

*The **OGE** (Office of Government Ethics) needs to allow designated government employees (Annual & New Entrant) to electronically file their OGE Form 450 reports as well as allow OGE attorneys to electronically review and certify the reports. OGE Form 450 reports are required to be stored in GSA record manager EDMS.*

***The OGE eForm 450 Phase 2 System** is a new web application that supports the employees to file the form 450 online and manage the life cycle of the Form 450 workflow.*

***Integration:** The OGE eForm 450 Phase 2 system will integrate with EDMS as a consumer and has no dependency on the DSS (Digital Signature Solution) system.*

The following types of PII will be corrected:

- *Employee name, agency, branch, grade, position, outside positions*
- *Contact information (e.g., address, telephone number, email address);*
- *Financial Information (assets and income, liabilities);*
- *Agreements and Arrangements*
- *Gifts and Travel Reimbursements*

PII Data Storage:

PII data collected by the system will be managed and stored in an encrypted MySQL database that is managed by the GSA DMT team. Records of 450 reports with PII information will also be stored in the GSA EDMS repository that is encrypted.

PII Data End to End Life Cycle:

GSA employees will need to login to the OGE eForm 450 system using standard GSA SSO or MFA authentication. An employee (filer of Form 450 report) will enter Form 450 information that includes PII through the web site and submit the report to Admin Support and Review Attorney to review and certify. The intermediate data and final records will be saved to the eForm 450 application database as well as GSA record management system EDMS. The eForm 450 database and the EDMS are encrypted and only authorized administrators can have access to the data. All records will be preserved for a minimum of 7 years unless a specific request is received from the GSA OGC office to purge the record.

The Admin Supports and Review Attorneys can view the reports by logging to the OGE eForm 450 system using standard GSA SSO or MFA authentication. After the reports are certified, the final records can no longer be modified and will be saved to the eForm 450 application database as well as GSA record management system EDMS.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

Executive branch agencies are required to submit an annual report to the United States Office of Government Ethics (OGE) concerning certain aspects of their ethics programs (Section 402(e)(1) of the Ethics in Government Act of 1978, as amended).

*The GSA **OGE** (Office of Government Ethics) required designated government employees (Annual & New Entrant) to electronically file their OGE Form 450 reports based on the positions of the employees.*

*GSA relies on OGE **SORN** OGE/GOVT-2 Executive Branch Confidential Financial Disclosure Reports for Privacy Act converge of this collection. SORN history: 84 FR 47301 (9/9/2019)*

1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?

OGE eForm 450 system will not provide search capability by user interface to any users of the system when it goes live on October 1, 2020. Only the Database Administrator of GSA MySQL team or system administrators of the system with special privilege can access the data using database interfaces. The administrator of EDMS or MySQL team will technically be able to search records if they choose to. OGE is no exception. GSA EDMS will store records of historical Form 450 reports in its encrypted and secured repository. Only people granted special privileges can view the records. GSA OGC Office must submit an official request to both OGC and EDMS teams to add a new personnel who will have access to the OGE 450 records on the EDMS.

1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

The paper Form 450 was approved under OMB No. 3209-0006.

There is an existing OGE eForm 450 Phase I project that has been in production since December 2019. The OGE eForm 450 Phase 2 project under development intended to be a replacement of the existing system. Both systems collect identical data for the GSA OGE as a paper Form 450.

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

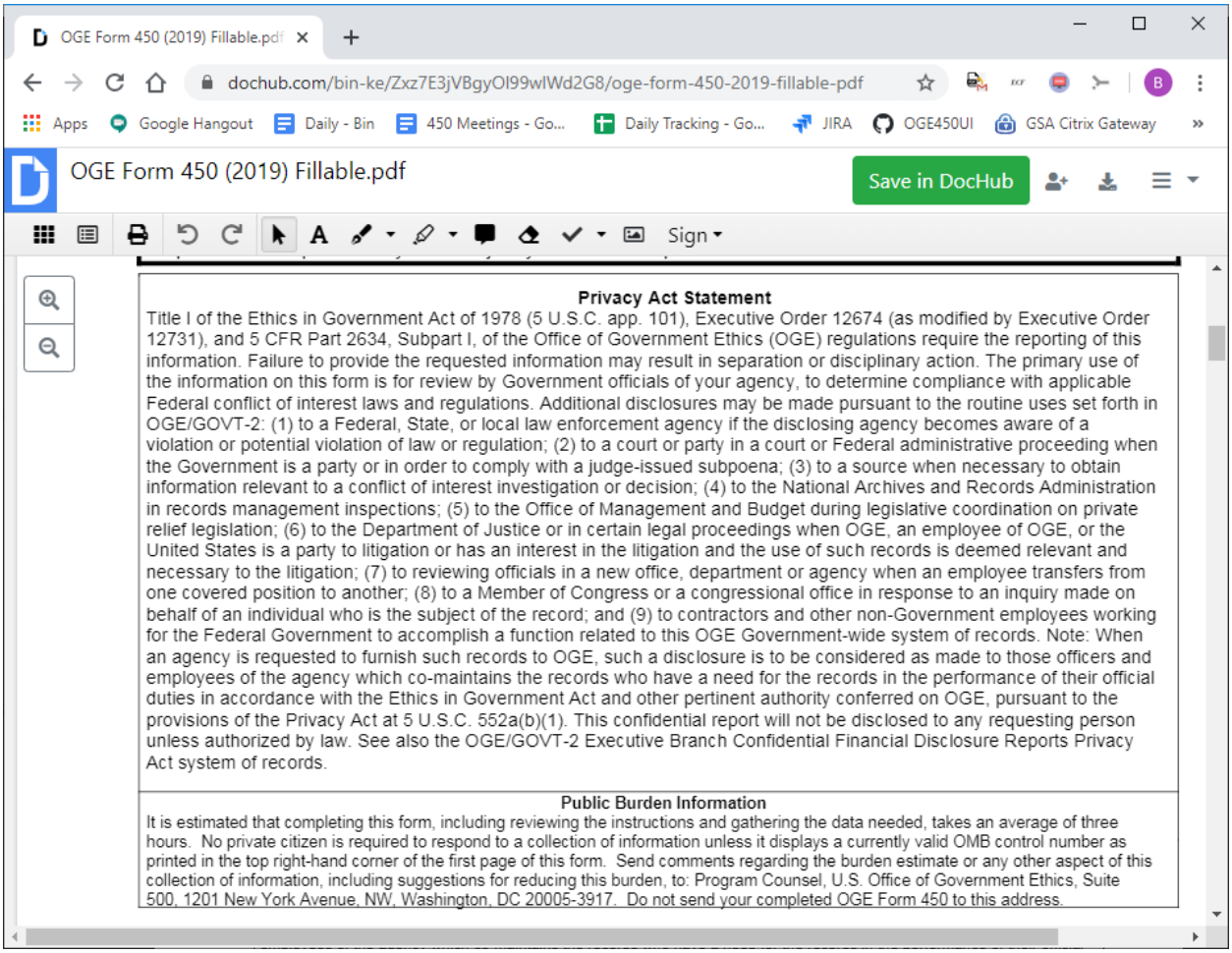
GSA OGE required the records to be preserved for seven years minimum. No records retention schedule approved by NARA.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

The system displays the below "Privacy Act Statement" to the filer before the filer starts Form 450 filing.



SECTION 3.0 DATA MINIMIZATION

GSA limits PII collection only to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

Executive branch agencies are required to submit an annual report to the United States Office of Government Ethics (OGE) concerning certain aspects of their ethics programs (Section 402(e)(1) of the Ethics in Government Act of 1978, as amended).

*The GSA **OGE** (Office of Government Ethics) required designated government employees (Annual & New Entrant) to electronically file their OGE Form 450 reports based on the positions of the employees.*

Prior to 2019, employees had submitted paper Form 450. There is an existing OGE eForm 450 Phase I project that has been in production since December 2019 to collect the Form 450 information in electronic format. The OGE eForm 450 Phase 2 project under development intended to be a replacement of the existing system. Both systems collect identical data for the GSA OGE according to OMB No. 3209-0006.

3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

No aggregated new data for an individual will be created by the system.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

The system will keep the Form 450 reports for each year without consolidation.

3.4 Will the system monitor the public, GSA employees, or contractors?

The system will not locate or monitor an individual.

3.5 What kinds of report(s) can be produced on individuals?

The system will not generate a report for an individual.

3.6 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

The system will not use any PII data for any reports generated by the system.

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

The system only collects data needed for the Form 450. No other data will be collected.

4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?

Only GSA OGE and approved GSA employees will have access to the system. The system will not share data with any other parties including other individuals, federal or state agencies or private organizations.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

The system collects the data from the individual directly only.

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

The system will integrate with GSA EDMS which is the GSA record manager. The system will store or retrieve documents from EDMS using the https protocol. Once the reports submitted by the individual has been approved by the review attorney, a copy of the report in PDF format along with any attachment will be sent and stored in the GSA EDMS repository by invoking rest APIs provided by the EDMS. The interaction between the system and the EDMS is under the established rules for GSA record management. There is no specific MOU between the project and the EDMS.

No data is shared externally by the system.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

The system collects the data from the individual directly only. The filer will fill up the Form 450 information on the system. All submitted data will be reviewed by Administration Support and the review attorneys to ensure that the data is complete and meet the standard of OGE Form 450.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

Only GSA employees approved by GSA OGE can access the system using SSO or MFA security protocol for authentication. There are three types of users to the system: Filer, Admin Support and Review Attorney. The users will be maintained and provided by the GSA OGE to the System Administrators.

Filer individual can login to the system to file the form 450 report and submit the report for review. The individual can only access and view only own Form 450 report.

Admin Support individuals can login to the system and view the submitted reports from the filers under the regions of the Admin Support individuals. Admin Support individuals can assign the report to a review attorney for review. Admin Support individual cannot access or view submitted reports from the filers outside the regions of the Admin Support.

Review attorney individuals can review and update the submitted reports assigned to them by the Admin Support. Review attorney individuals cannot access reports not assigned to them.

The Administrator of the system can have access to all the data in the database of the system.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

The System Security Plan (SSP) has been completed and is currently under review by ISSO. ATO is expected to be granted prior to 12/1/2020.

6.3 How will the system or application be secured from a physical, technical, and managerial perspective?

Only GSA employees approved by GSA OGE can access the system using SSO or MFA security protocol for authentication.

Collected data will be stored in the encrypted database server that is under the management of the GSA MySQL team that meets the high-level security requirement.

Report records will also be stored in the GSA EDMS repository that is an encrypted environment that meets the high level security requirement.

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

For any security incident, the issue will be reported to the product owner and the GSA OGE immediately. Problem tracing and remedy will be done with the highest priority that involves any resources or teams necessary.

In addition, the staff follows the GSA Incident Response Procedural Guide (CIO IT Security 01-0) to report and respond to any identified security incidents pertaining to PII.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

The duties and responsibilities of the employee position require the employee to file the Confidential Financial Disclosure Report to avoid involvement in a real or apparent conflict of interest. The purpose of Form 450 report is to assist employees and their agencies in avoiding conflicts between official duties and private financial interests or affiliations. The information will only be used for legitimate purposes, and will not be disclosed to any requesting person unless authorized by law.

The system will display "Privacy Act Statement" to the filer before the filer starts Form 450 filing. Only GSA employees identified by the GSA OGE are required to fill out the Form

450 on the system. The individual can reach out and discuss with GSA OGE if the person have questions or concerns filing the form.

7.2 What procedures allow individuals to access their information?

Email notices will be sent to GSA employees identified by the GSA OGE who are required to fill out the Form 450 on the system. The system will display "Privacy Act Statement" to the filer before the filer starts Form 450 filing.

7.3 Can individuals amend information about themselves? If so, how?

After a filer submits the Form 450 through the system, the filer can update or correct the information in the submitted report. Once the report is reviewed and certified by the review attorney, the filer or any other individuals will no longer be able to change any information of the report. The filer will need to contact the Admin Support of GSA OGE to address any issues.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

All GSA users must take security privacy and awareness training as well as role-based privacy training on an annual basis.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system owner ensure that the information is used only according to the stated practices in this PIA?

The system has auditing logging that will record any data changes made to a record If not the individual. The audit logging will be permanently preserved by the system. Individual users can access the system based on the roles. The system owner will be able to audit

the system if requested. For every form 450 submitted by a GSA employee (filer), only the authorized Admin Support and review attorney can view and access the submitted form. The authorization had been implemented by the system. The system will also keep track of any changes made by an individual other than the filer by database logging of the changes.

---

[1] OMB Memorandum *Preparing for and Responding to the Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.