



## Privacy Office Contact Information

Please send any questions by email to [gsa.privacyact@gsa.gov](mailto:gsa.privacyact@gsa.gov) or by U.S. Mail to:  
General Services Administration  
Chief Privacy Officer  
1800 F Street NW  
Washington, DC 20405

## Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, 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]

[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.

## General Information

PIA Identifier: 349  
System Name: OGE eForm 450  
CPO Approval Date: 5/9/2022  
PIA Expiration Date: 5/8/2025

## Information System Security Manager (ISSM) Approval

Nathaniel Ciano

## System Owner/Program Manager Approval

Chris McFerren

## Chief Privacy Officer (CPO) Approval

Richard Speidel

## PIA Overview

**A:** System, Application, or Project Name:  
OGE eForm 450

**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:

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

## Overview:

The GSA **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. **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. The final certified OGE Form 450 reports are required to be stored in GSA record manager Electronic Document Management Software (EDMS) as records. The application is on-premises, will be accessed by authorized internal GSA and will not be available outside the GSA Domain.

The eForm450 application has two user sets that access via different authentication methods.

The first is the GSA OGE approved application user set, the other, Privileged Accounts, are reserved for those users with an active SNA and have been granted permission to access the eForm450 on the application back-end level. For GSA employees who are the approved users of the eForm450 application, the users will access the application using a GSA laptop with PIV card. The authentication is done using GSA SSO which was implemented using GSA SecureAuth.

For privileged accounts, the users first need to login to GSA network using MFA (PIV and Pin) using VPN. Once the users login to GSA internal network, the users can use ID and Password to login to the approved servers with MFA through the Citrix VDI. For access to MySQL servers, the users must login to Citrix system first to use SSH and Putty to login to the MySQL servers.

**Integration:** The OGE eForm 450 Phase 2 system will integrate with GSA Electronic Document Management Software (EDMS).

## 1.0 Purpose of Collection

**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?  
No

**1.2a:** If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?

**1.2: System of Records Notice(s) (Legacy Text):** 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.

---

**1.2b:** Explain why a SORN is not required.

**1.3:** Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

**1.3: Information Collection Request:** 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:** What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.

Records are maintained and verified while an employee has active employment. After a user leaves GSA, the email record will be available for 7 years and 15 years for high level officials. Records are disposed of as specified in the handbook, GSA Records Maintenance and Disposition System (CIO P 1820.1). The record retention period is indefinite; this is part of GSA Number/Disposition Authority GRS 03.1/011 and DAAGRS-2013-0005-0008.

## **2.0 Openness and Transparency**

**2.1:** Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

**2.1 Explain:** If not, please explain.

## **3.0 Data Minimization**

**3.1:** Why is the collection and use of the PII necessary to the project or system?

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. DocuSign Envelope ID: 472ACA5F-92B2-4887-85ED-262665585C70 12 Version 3.0: September 24, 2020 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?

No

**3.2 Explained:** 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?

None

**3.4 Explain:** Please elaborate as needed.

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?

---

No

**3.6 Explain:** If so, what process(es) will be used to aggregate or de-identify the data?

**3.6 Why Not:** Why will the data not be de-identified?

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

#### **4.0 Limits on Using and Sharing Information**

**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?

Yes

**4.2:** Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?

Federal Agencies

**4.2How:** 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

**4.3Other Source:** What is the other source(s)?

**4.4:** Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?

Yes

**4.4WhoHow:** If so, who and how?

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.

**4.4Formal Agreement:** Is a formal agreement(s) in place?

No

**4.4NoAgreement:** Why is there not a formal agreement in place?

No data is shared externally by the system

#### **5.0 Data Quality and Integrity**

**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.

#### **6.0 Security**

**6.1a:** Who or what will have access to the data in the system, application, or project?

---

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.

**6.1b:** What is the authorization process to gain access?

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 a System Security Plan (SSP) been completed for the Information System(s) supporting the project?

Yes

**6.2a:** Enter the actual or expected ATO date from the associated authorization package.

5/10/2022

**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?

Yes

**6.4What:** 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.

## **7.0 Individual Participation**

**7.1:** What opportunities do individuals have to consent or decline to provide information?

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 DocuSign Envelope ID: 472ACA5F-92B2-4887-85ED-262665585C70 16 Version 3.0: September 24, 2020 450 on the system. The individual can reach out and discuss with GSA OGE if the person have questions or concerns filing the form.

**7.1Opt:** Can they opt-in or opt-out?

No

**7.1Explain:** If there are no opportunities to consent, decline, opt in, or opt out, please explain.

**No opportunities exist to consent, decline or opt out. Sources may vary widely as information is not collected by the system's applications specifically, but are used as a mechanism to store, collaborate and share information between users**

**7.2:** What are the procedures that 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?

Yes

**7.3How:** How do individuals amend information about themselves?

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.

## **8.0 Awareness and Training**

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

GSA requires annual privacy, security training & collaboration sharing for all personnel and has policies in place that govern the proper handling of PII. This is managed through the CIO and Online Learning University (OLU) system.

## **9.0 Accountability and Auditing**

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

GSA requires privacy and security training for all personnel, and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, including those that support design research, and has limited access to those personnel with a need to know. Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. As discussed above, GSA takes automated precautions against overly open access controls.

---