Privacy Office Contact Information

Please send any questions by email to 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: 437
System Name: FOIA Case Management System (FOIAXpress)
CPO Approval Date: 6/28/2023
PIA Expiration Date: 6/27/2026

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:
FOIA Case Management System (FOIAXpress)

B: System, application, or project includes information about:
FOIAXpress complies with eFOIA regulations, provides mandated Dept. of Justice reports and keeps track of metrics and fees associated with processing the agency's FOIA requests.

C: For the categories listed above, how many records are there for each?
56,000 Records

D: System, application, or project includes these data elements:
Contact Information: First name and Last name, personal email address, and phone number (could be personal or business).

Business Information: Business email address, name of the business or company.

Overview:

FOIAXpress is a commercial-off-the-shelf, based on the eCase adaptive for case management, solution developed for federal agencies to manage the Freedom of Information Act (FOIA) request life-cycle. This solution complies with eFOIA regulations, provides mandated Dept. of Justice reports and keeps track of metrics and fees associated with processing the agency's FOIA requests.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The following legal authorities apply:

Freedom of Information Act, 5 U.S.C. 552; Privacy Act of 1974 as amended, 5 U.S.C. 552a; 5 U.S.C. 301, and 44 U.S.C. 3101.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

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

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
GSA/OGC-1

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.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
GSA maintains electronic and paper records in accordance with published National Archives and Records Administration (NARA) Disposition Schedule, Transmittal No. 31, and General Records Schedule (GRS) 4.2, Information Access and Protection Records. Records pertaining to FOIA and Privacy Act programs are retained and disposed of in accordance with the GRS 4.2.
Files created in response to requests for information under the FOIA, consisting of the original request, a copy of the reply, and all related supporting files
which may include the official file copy of the requested records or copies thereof. For FOIA requests for accessioned records, see file no. 1422, "FOIA and
Mandatory Review Request Files."
Correspondence and supporting documents (EXCLUDING the official file copy of the records requested if filed herein). See file no. 1010 for FOIA appeals
files.
a. Granting access to all of the requested records.
b. Responding to: requests for nonexistent records, requesters who provide inadequate descriptions, and those who fail to pay NARA reproduction fees.
c. Denying access to all or part of the records requested.

Temporary
Use GRS_4-2-020

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?
PII from the information collected is used to track, search, and respond back to a request or requester. FOIAXpress also collects name, email address, username, and password from Federal employees and contractors to create their user profiles.

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?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
All employees, including those that maintain this application, are required to take annual cybersecurity and privacy awareness training. Also, system training for new users is provided by the vendor. Rules of behavior guidelines are adhered to for user access. All communication flows are encrypted. System access is limited to authorized account holders.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
This system is not a monitoring tool. The system is used to provide feedback to requesters.

3.5 What kinds of report(s) can be produced on individuals?
There are various reports that can be produced such as requester reports, quarterly reports and annual reports. The reports are dependent on how GSA's version of FOIAXpress is configured.

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
Yes, most reports will be de- identified. Reports are searchable by field. Only requestor reports will have PII but access is limited to those reports.

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

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?
GSA shares information collected for FOIA requests with other federal agencies via emails for consultations and referrals. Also, requester names are released to the public in our FOIA logs, but logs are pulled by time frame (ex: requests received in April 2022), not by individual. If the files are larger, they are encrypted on a thumb drive and sent through USPS or FedEX to the designated agency.

Other agencies will receive a copy of the request, plus the responsive records. They will either review the record and provide suggested redactions feedback. Or they will enter the request into the system and process the records. In both instances, the other agency will be taking the requester's basic info (name and contact) and very likely putting it in their FOIA tracking system (whichever one they use).

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?
No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
This is not applicable. The system does not interact with other system and so an SLA or MOU is not required at this time.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
Individuals submitting requests are responsible for ensuring that the information they submit is accurate. GSA personnel review potentially responsive records and confirm that the information in the records match the information requested.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Only authorized GSA FOIA personnel will have access to the data supplied by requesters via FOIAXpress.

6.1b: What is the authorization process to gain access?
Access to the system is granted based on SSO for all GSA users and Login.gov on the Public Access Link for the general public.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
No

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

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Physical controls are in place and only approved personnel have access to the datacenter. Approved personnel have badges to enter the facility. Security controls like biometrics, 24/7 monitoring are in place. All the systems are logically separated and each agency is logically separated with their own vLAN (subnet).

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?
Alerts will be generated from firewall for any IPS detections and log analyzer tools generate alerts for any unusual activity. Should a security breach occur, the GSA IR team will be alerted.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
All information provided by FOIA/PA requesters to GSA is voluntary. Requesters may freely decline to provide any information they do not wish to provide; however, such a refusal may adversely affect GSA's ability to process a FOIA or PA response if the contact information is inadequate or the individual's identity cannot be authenticated.

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

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

7.2: What are the procedures that allow individuals to access their information?
The requestor creates an account, they are able to review their request after it is submitted in PAL. This is all dependent on the configuration.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

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.
All GSA users are mandated to take annual privacy training on OLU. All users take part in the FOIAXpress training before they can use the system. For Public Access Link (PAL), there is no public training. Individuals will be prompted with a Privacy Act Statement on PAL.

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?
The system owner will ensure that the information is used only according to the stated practices in this PIA through proper system administration to include account management with the application of role-based access controls.