



U.S. DEPARTMENT OF LABOR
Office of the Chief Information Officer



PRIVACY IMPACT ASSESSMENT
FOIAXPRESS

VERSION 1.3

01/29/2024

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
03/20/2020	Privacy Impact Assessment 1.0	Benjamin Asirifi	Initial Draft
03/23/2020	Privacy Impact Assessment 1.1	Benjamin Asirifi	Final Draft
1/8/2021	Privacy Impact Assessment 1.2	Khani Heath	FY21 Update
1/29/2024	PIA 1.3	System Team/ISSO	FY24 Updates

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
03/23/2020	Privacy Impact Assessment	Thomas Giancola and the OPEXUS team
1/8/2021	Privacy Impact Assessment	Adrienne Ramirez
1/29/2024	PIA	System Team/ISSO

TABLE OF CONTENTS

Privacy Impact Assessment Questionnaire	4
1.1 Overview	4
1.2 Characterization of the Information	5
1.3 Describe the Uses of the PII.....	6
1.4 Retention	7
1.5 Internal Sharing and Disclosure	8
1.6 External Sharing and Disclosure	9
1.7 Notice	10
1.8 Individual Access, Redress, and Correction.....	11
1.9 Technical Access and Security.....	11
1.10 Technology.....	13
1.11 Determination.....	14
1.12 PIA Signature Page	15
Appendix A: Definition for PII and PII Elements.....	15

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1 OVERVIEW

Freedom of Information Act (FOIA) Xpress a Commercial Off - The Shelf (COTS) application owned by the Department of Labor (DOL) Office of the Assistant Secretary for Administration and Management (OASAM).

FOIAXpress is a Software as a Service (SaaS) that is managed by OPEXUS and is maintained in accordance with the provisions of the Freedom of Information Act, 5 USC 552, which requires that each agency shall: establish a system to assign an individualized tracking number for each request received that will take longer than ten days to process and provide to each person making a request the tracking number assigned to the request; and establish a telephone line or Internet service that provides information about the status of a request to the person making the request using the assigned tracking number, including, the date on which the agency originally received the request and an estimated date on which the agency will complete action on the request. The mission for FOIAXpress. In addition to FOIAXpress, DOL has acquired the Public Access Link (PAL), Electronic Document Review (EDR) and Collaboration Portal.

- PAL: Integrated web-based application via which the public can submit requests and track and receive responses
- EDR: speeds the document review and discovery process
- Collaboration Portal: allows non-users of FOIAXpress to locate responsive documents and work with FOIA staff on requests

FOIAXpress processes Personally Identifiable Information (PII) in the form of names, mailing address, telephone numbers, personal email address and business physical address. FOIAXpress automates the full lifecycle of Freedom of Information Act (FOIA) requests and appeals – from initial inquiry to delivery of documents through archival of the case. This system is used to document and track the status of requests made by the public under FOIA and the Privacy Act (PA) for documents maintained by the Department. The PAL component is the public-facing web portal that complements FOIAXpress to provide efficient and secure communication between citizens and agencies, public can submit requests and track and receive responses. The EDR speeds the document review and discovery process. The Collaboration Portal allows non-users of FOIAXpress to locate responsive documents and work with FOIA staff on requests. The Freedom of Information Act, 5 USC 552, The Privacy Act of 1974, Office of Management and Budget (OMB) Circular A-130, and OMB M-99-18, “Privacy policies on Federal Web sites” Due to the collection of personal data, any disclosure of data would constitute an unwanted invasion and personal privacy.

This PIA is being updated because the system contains PII information from the public. The PAL feature is a public-facing web portal that complements the FOIAXpress system by providing efficient and secure communication between agencies and the public. The PAL feature allows members of the public to submit and track the status of requests and receive responses directly through the FOIAXpress web portal.

1.2 CHARACTERIZATION OF THE INFORMATION

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, or technology being developed.

Specify whether the System collects personally identifiable information (PII) on DOL employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children.

- From whom is information to be collected?

The information collected is from members of the public (US citizens)

- Why is the Information being collected?

The information collected in the system is used to respond to access requests under the FOIA or the PA, to track these requests in order to maintain compliance with statutory response times, and to maintain documents responsive to these requests, regardless of whether they are exempt from disclosure to the requester under the FOIA or the Privacy Act.

- What is the PII being collected, used, disseminated, or maintained? Name, phone number, mailing address, personal email and business name, business email, business physical address.

- How is the PII collected?

The PII is collected online through PAL. This is an integrated web-based application via which the public can submit requests, track and receive responses

- How will the information collected from individuals or derived from the system be checked for accuracy?

The PAL component is the public-facing web portal that complements FOIAXpress to provide efficient and secure communication between citizens and agencies, public can submit requests and track and receive responses. The EDR speeds the document review and discovery process

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?

The Privacy Act of 1974, Office of Management and Budget (OMB) Circular A-130, and OMB M-99-18, "Privacy policies on Federal Web sites" Due to the collection of personal data, any disclosure of data would constitute an unwanted invasion of personal privacy.

- Privacy Impact Analysis

The main privacy risk associated with the collection and maintenance of PII in the system is about FOIA and PA requesters is that individual requesters may, when filing their access request, include sensitive personal information about themselves, or about other individuals in their

request. Similar risks are presented by the entering of responsive documents into the system. This information could then be compromised by unauthorized access or disclosure. To mitigate these risks, the DOL FOIA and PA has taken steps to minimize the amount of information that the agency collects and maintains while processing requests. For example, the PAL feature only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests; the DOL FOIA offices do not ask requesters to provide sensitive information (e.g., Social Security numbers). If the user declines to provide this information, the system does not grant access. The user has no right or opportunity to decline to provide other usage data in the system (e.g., date, time of user session), which is generated and maintained automatically by the system itself. To avoid unauthorized access or disclosure, this information is logged into the database, but system access is limited (by software licenses) to a small number of specified DOL professionals who need system access to do their jobs.

1.3 DESCRIBE THE USES OF THE PII

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

- Describe all the uses of the PII

The information collected in the FOIAXpress system is used to respond to requests under FOIA or the PA, to track these requests in order to maintain compliance with statutory response times, and to maintain documents responsive to these requests in compliance with legal retention and disposition schedules, including any records that are exempt from disclosure to the requester under FOIA or the PA.

- What types of tools are used to analyze data and what type of data may be produced?

Below are the tools that will be used:

- PAL: Integrated web-based application via which the public can submit requests and track and receive responses
- EDR: speeds the document review and discovery process
- Collaboration Portal: allows non-users of FOIAXpress to locate responsive documents and work with FOIA staff on requests

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?

No.

- If the system uses commercial or publicly available data, please explain why and how it is used.

No.

- Will the use of PII create or modify a “system of records notification” under the Privacy Act?

Yes, a System of Records Notification (SORN) will be created and published for this system

- Privacy Impact Analysis

The main privacy risk associated with the collection and maintenance of PII in the system about FOIA and PA requesters is that individual requesters may, when filing their access request, include sensitive personal information about themselves, or about other individuals in their request. Similar risks are presented by the entering of responsive documents into the system. This information could then be compromised by unauthorized access or disclosure. To mitigate these risks, the DOL FOIA and PA has taken steps to minimize the amount of information that the agency collects and maintains while processing requests. For example, the PAL feature only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests; the DOL FOIA offices do not ask requesters to provide sensitive information (e.g., Social Security numbers). If the user declines to provide this information, the system does not grant access. The user has no right or opportunity to decline to provide other usage data in the system (e.g., date, time of user session), which is generated and maintained automatically by the system itself. To avoid unauthorized access or disclosure, this information is logged into the database, but system access is limited (by software licenses) to a small number of specified DOL professionals who need system access to do their jobs.

1.4 RETENTION

The following questions are intended to outline how long information will be retained after the initial collection.

- What is the retention period for the data in the system?

Records are retained and disposed of in accordance with General Records Schedule 14, issued by the National Archives and Records Administration (NARA), and other applicable schedules approved or issued by NARA. Additionally, FOIAXpress will verify whether any open appeal or litigation matters exist for the closed request. In such instances, the system will not allow users to mark the request for deletion.

- Is a retention period established to minimize privacy risk?

Records are retained and disposed of in accordance with General Records Schedule 14, issued by the National Archives and Records Administration (NARA), and other applicable schedules approved or issued by NARA. Additionally, FOIAXpress will verify whether any open appeal or litigation matters exist for the closed request. In such instances, the system will not allow users to mark the request for deletion.

- Has the retention schedule been approved National Archives and Records Administration (NARA)? Provide the retention schedule number for the schedule utilized?
FOIAXpress records retention schedule have been approved by the DOL Records Officer and filed with NARA.
- Per M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?
FOIAXpress collects minimal PII data and that is being assessed annually for applicability and will be eliminated if not required by business functions.

- Have you implemented the DOL PII Data Extract Guide for the purpose of eliminating or reducing PII?

Yes, FOIAXpress collects minimal PII data and that is being assessed annually for applicability and will be eliminated if not required by business functions.

- How is it determined that PII is no longer required?

These are requirement within the system and PII is always required however, a privacy threshold assessment is performed annually to ascertain if PII is no longer required for responding to inquiries.

- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.

PII information is not masked or anonymized. PII information is only accessible by authorized users.

- Privacy Impact Analysis

The main privacy risk associated with the collection and maintenance of PII in the system about FOIA and PA requesters is that individual requesters may, when filing their access request, include sensitive personal information about themselves, or about other individuals in their request. Similar risks are presented by the entering of responsive documents into the system. This information could then be compromised by unauthorized access or disclosure. To mitigate these risks, the DOL FOIA and PA has taken steps to minimize the amount of information that the agency collects and maintains while processing requests. For example, the PAL feature only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests; the DOL FOIA offices do not ask requesters to provide sensitive information (e.g., Social Security numbers). If the user declines to provide this information, the system does not grant access. The user has no right or opportunity to decline to provide other usage data in the system (e.g., date, time of user session), which is generated and maintained automatically by the system itself. To avoid unauthorized access or disclosure, this information is logged into the database, but system access is limited (by software licenses) to a small number of specified DOL professionals who need system access to do their jobs.

1.5 INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

- With which internal organization(s) is the PII shared, what information is shared, and for what purpose?

The PII collected is shared internally with other organizations strictly for the purpose of responding to the requester.

- How is the PII transmitted or disclosed?

PII is transmitted digitally within the system using TLS encryption.

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?

An privacy threshold assessment is performed annually to ascertain if PII is no longer required for responding to inquiries.

- Privacy Impact Analysis

There is no privacy impact to internal sharing of data.

1.6 EXTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the content, scope, and authority for information sharing external to DOL which includes federal, state and local government, and the private sector.

- With which external organization(s) is the PII shared, what information is shared, and for what purpose?
PII is not shared with any external organization
- Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, provide the SORN ID in use for this system.. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.
PII is not shared with any external organization
- How is the information shared outside the Department and what security measures safeguard its transmission?
PII is not shared with any external organization
- How is the information transmitted or disclosed?
N/A
- Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If the answer is yes, be prepared to provide a copy of the agreement in the event of an audit as supporting evidence.
N/A
- How is the shared information secured by the recipient?
PII is not shared with any external organization
- What type of training is required for users from agencies outside DOL prior to receiving access to the information?

N/A

- Privacy Impact Analysis
N/A

1.7 NOTICE

The following questions are directed at notice to the individual of the scope of PII collected, the right to consent to uses of said information, and the right to decline to provide information.

- Was notice provided to the individual prior to collection of PII? If yes, please provide a copy of the notice as an appendix or be prepared to provide a copy of the notice during an audit request. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, please explain.
Yes, notice is provided on the PAL tool.
- Do individuals have the opportunity and/or right to decline to provide information?
Yes, individuals have the opportunity to decline to provide information but won't be able to submit and track request status
- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
The public has been made aware, through formal publication, of the types of information collected and routine uses that will be made of the information collected under DOL/OASAM-24 — Privacy Act/Freedom of Information Act Requests File System. An individual, armed with that knowledge, may decide whether or not to correspond with the Department or submit a FOIA request. The decision to do so is voluntary.
- Privacy Impact Analysis
There is no privacy impact to providing notification

1.8 INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

- What are the procedures that allow individuals to gain access to their own information?
None – members of the public do not have direct access to the system. Information from the system may be made available, consistent with Federal law, in response to a request for such information.
- What are the procedures for correcting inaccurate or erroneous information?
As appropriate, any corrections are done per individual's request, consistent with the provisions of the Privacy Act and DOL's implementing regulations.
- How are individuals notified of the procedures for correcting their own information?
If system user finds information that requires correction, notification may occur in writing, via fax, mail, or e-mail, to the requestor of the information. For records subject to the provisions of the Privacy Act, notification procedures are provided in the SORN and in DOL's regulations.
- If no formal redress is provided, what alternatives are available to the individual?
There is no formal redress or alternate process available as the information is voluntarily submitted. If additional information is needed the individual is contacted and erroneous data is corrected at that time. For records subject to the provisions of the Privacy Act, redress procedures are provided in the SORN and in DOL's regulations.
- Privacy Impact Analysis
There is no additional risk in redress process as the public does not have direct access.

1.9 TECHNICAL ACCESS AND SECURITY

The following questions are intended to describe technical safeguards and security measures.

- Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)
To avoid unauthorized access or disclosure, this information is logged into the database, but system access is limited (by software licenses) to a small number of specified DOL professionals who need system access to do their jobs. These users are responsible for the processing of FOIA requests at DOL (FOIA analysts, supervisors, etc.).
- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA or be prepared to provide copies during an audit request.

Contractors will have access to FOIAXpress

- Does the system use “roles” to assign privileges to users of the system? If yes, describe the roles.
Access to view PII data is based on a user’s role and need to know.
- What procedures are in place to determine which users may access the system and are they documented?
There will be an SOP documenting the procedures in place.
- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided? Provide date of last training.
Annual Cybersecurity and Privacy Awareness Training will be provided to all DOL FOIAXpress users as documented within the Computer Security Handbook.
- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?
Annual Privacy Training aka Cybersecurity and Privacy Awareness will be provided to all DOL FOIAXpress users as documented within the Computer Security Handbook.
- What auditing measures and technical safeguards are in place to prevent misuse of data?
 - Username and passwords are used to authenticate users
 - Access to view student or other data is based on a user’s role and need to know
 - All data is encrypted
 - The OPEXUS platform audits the use of privileged functions
- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?
FOIAXpress data is secured according to the FISMA requirements. FOIAXpress is now going through the Assessment and Authorization process, so date will be TBD.
- Privacy Impact Analysis
The main privacy risk associated with the collection and maintenance of PII in the system about FOIA and PA requesters is that individual requesters may, when filing their access request, include sensitive personal information about themselves, or about other individuals in their request. Similar risks are presented by the entering of responsive documents into the system. This information could then be compromised by unauthorized access or disclosure. To mitigate these risks, the DOL FOIA and PA has taken steps to minimize the amount of information that the agency collects and maintains while processing requests. For example, the PAL feature only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests; the DOL FOIA offices do not ask requesters to provide sensitive information (e.g., Social Security numbers). System users must enter their user ID and passwords (in the login screen) in order to be given access to the FOIAXpress system. If the user declines to provide this information, the system does not grant access. The user has no right or opportunity to decline to provide other usage data in the system (e.g., date, time of user

session), which is generated and maintained automatically by the system itself. To avoid unauthorized access or disclosure, this information is logged into the database, but system access is limited (by software licenses) to a small number of specified DOL professionals who need system access to do their jobs. Each user must have a valid and current password. Only the user and other designated FOIA professionals with Administrator rights can change these passwords.

1.10 TECHNOLOGY

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, biometrics, and other technology.

- Was the system built from the ground up or purchased and installed?
The application is being developed to replace the legacy system SIMS-FOIA. FOIAXpress will be provided as a SaaS solution from OPEXUS Cloud Service Provider (CSP).
- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.
Data integrity, privacy, and security are an integral part of every step of the system development process. The criteria for choosing the vendor who developed the system included experience in developing data secure systems. From secure system login to encryption of data at rest to use restricted to secure facility, every aspect of FOIAXpress and its use is focused on data integrity, privacy, and security.
- What design choices were made to enhance privacy?
Communication is secured using encryption, PII data is also encrypted at rest. FOIAXpress/PAL stores the data in SQL Server which is encrypted using TDE encryption.
- For systems in development, what stage of development is the system in, and what project development life cycle was used?
At OPEXUS, an agile methodology and sprint-based development and testing is being used for product releases. One major and one minor release of FOIAXpress is done every year. Hot fixes will be released on demand. All the feature requests and issues are added to product backlog and considered for future releases. Backlogged items are reviewed before planning our major and minor releases.
- For systems in development, does the project employ technology that may raise privacy concerns? If so, please discuss their implementation?
No technology of concern is used. Communication is secured using encryption, PII data is also encrypted at rest.

1.11 DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

DOL has completed the PIA for FOIAXpress which is currently in development. DOL has determined that the safeguards and controls for this moderate system will adequately protect the information and will be referenced in FOIA System Security Plan to be completed by May 2020

DOL has determine that it is collecting the minimum necessary information for the proper performance if a documented agency function.

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business physical address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements, increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained?
Also, note whether the collection is for ☒ Federal employees, ☒ Contractor staff, ☒ Members of the Public {Check all that apply}

- ☐ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr. ☐
- ☒ First name ☒ Middle initial and/or ☒ Last name
- ☐ Name suffix such as Jr. Sr., etc.
- ☐ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☐ SSN
- ☐ SSN [truncated]
- ☐ SSN [elongated]
- ☐ Language spoken
- ☐ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license plate, VIN)
- ☐ Driver's license number
- ☒ Residential address
- ☒ Personal phone numbers (e.g., phone, fax, cell)
- ☒ Mailing address (e.g., P.O. Box)

- ☒ Personal e-mail address
- ☒ Business address
- ☒ Business phone number (e.g., phone, fax, cell)
- ☒ Business e-mail address
- ☐ Medical information including physician's notes
- ☐ Medical record number
- ☐ Device identifiers (e.g., pacemaker, hearing aid)
- ☐ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- ☐ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- ☐ Certificates (e.g., birth, death, marriage)
- ☐ Legal documents or notes (e.g., divorce decree, criminal records)
- ☐ Educational records
- ☐ Network logon credentials (e.g., username and password, public key certificate)
- ☐ Digital signing or encryption certificate
- ☐ Other: _____
- ☐ None

- Is any part of the PII collection voluntary?

Yes, PII collection is voluntary

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?

PII information is not masked or anonymized. PII information is only accessible by authorized users