Privacy Impact Assessment (PIA)
for the

FOIAXpress in the Cloud
May 6, 2020

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Arthur Caliguiran/System Administrator
Contact Email: Arthur.Caliguiran@ed.gov

System Owner

Name/Title: Gregory Smith/ Director, FOIA Service Center
Principal Office: Office of the Secretary (OS)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Department of Education (the Department) utilizes a commercial off-the-shelf web-based system called FOIAXpress. This system is used to document and track the status of requests made under both the Freedom of Information Act (FOIA) and the Privacy Act (PA). Requests under FOIA may include requests for information or requests for review of initial denials. Requests under PA include requests for notification of the existence of records, access to records, amendment of records, accounting of disclosures of records and requests for review of initial denials of such requests for notification, access, and amendment. This system is also used to generate the annual and quarterly reporting statistics to the Department of Justice (DOJ) as required by the Freedom of Information Act.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

When an individual submits a request under FIOA or PA, they provide their contact information for the purposes of receiving a response from the Department. They may also include additional information in their request to authenticate their identity.

Additionally, when a FOIA or PA request is for documents or records that contain PII, prior to redaction of the PII and release of the record, a copy of the original document is maintained in the system for accounting purposes.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

Updated PIA

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Freedom of Information Act, 5 U.S.C. 552, as amended By Public Law No. 110-175, 121 Stat. 2524; OPEN Government Act of 2007 (S. 2488); The Privacy Act of 1974, 5 U.S.C. 552a, as amended; and 5 U.S.C. 301.

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

Freedom of Information Act and Privacy Act Tracking System (18-05-20) published in the Federal Register on May 29, 2015 at 80 FR 30671.

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

https://www.federalregister.gov/documents/2015/05/29/2015-13048/privacy-act-of-1974-system-of-records

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

Records relating to Freedom of Information Act and Privacy Act Tracking System are retained in accordance with the following schedules:

- Access and disclosure request files GRS 4.2 Item 020 (DAA GRS 2016 0002-0001). Temporary destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later.
- Accounting for and control of access to classified and controlled unclassified records and records requested under FOIA, PA, and MDR, GRS 4.2 Item 040 (DAA-GRS-2016-0002-0004). Temporary destroy or delete 5 years after date of last entry.
- Special purpose computer programs and applications, GRS 3.1, item 011((DAA-GRS-2013-0005-0008). Temporary 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

FOIAXpress collects the names, address(es), phone number, fax number, and email of the requester, dates of request and responses, descriptions or identifications of records requested, amount of fees paid, if any; payment delinquencies, if any; final determinations of appeals or denials and summary of log.

Data elements provided by an individual making a PA request may also provide a description of records being requested such as a complaint number or loan account number and date of birth and Social Security Number in order to certify identity.

Other PII may be maintained in FOIAXpress would be contained in records requested under FOIA or PA. This includes a wide range of possible PII but is limited to records the Department maintains that are subject to FOIA and PA.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

PII collected by FOIAXpress is provided directly by the individuals.

Additional PII maintained in FOIAXpress as part of a record requested under FOIA or PA would come from another information system within the Department.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

Information collected from individuals are received either in paper form, web page(https://foiaxpress.pal.ed.gov/app/Home.aspx), email, or fax. PII contained in a records requested under FOIA or PA would be uploaded to FOIAXpress prior to review and redaction.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Information on Privacy Act requests are validated with the information provided by the requester on the separate certification of identity form. This information is further validated when locating the records they are seeking notification, access, or amendment to.

For information provided on FOIA requests, the integrity of the information is ensured by the individual making a request under FOIA. Without proper contact information, the individual will not receive their requested information.

Additionally, PII maintained in FOIAXpress can be validated when a requester contacts the FOIA Service Center for follow ups.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The PII collected by FOIAXpress is used to track the status, search, and respond to FOIA and Privacy Act requests.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

When making a Privacy Act request, an individual must provide their SSN on the Certification of Identity and Consent to verify the identity of the individual prior to giving access to their records.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

No other alternatives were considered because the SSN is a unique identifier utilized to verify an individual's identity and ensure the correct records are accessed pursuant to a Privacy Act request.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

Notice is provided on all forms requesting PII that are submitted to the FOIA Service Center: FOIA Request Form, Privacy Act Request Form; and the Certification of Identity and Consent. Notice is also provided to individuals prior to creating an account on https://foiaxpress.pal.ed.gov/app/Home.aspx

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

FOIA Request Form: https://www2.ed.gov/policy/gen/leg/foia/foia-request-form.pdf
Privacy Act Request Form: https://www2.ed.gov/policy/gen/leg/foia/privacy-act-request.pdf
Certification of Identity and Consent: https://www2.ed.gov/policy/gen/leg/foia/certification-of-identity-and-consent.pdf

Additional notice is found here: https://foiaxpress.pal.ed.gov/app/CreateRequester.aspx

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

If the requester does not want to provide their information, they can decline to provide their information. However, this may result in their request not being processed.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

Click here to enter text.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

PII related to a requester may be shared with another Federal agency is a request is for records shared between the other agency and the Department.

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

The purpose of sharing would be to ensure a request is fulfilled appropriately.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☐ N/A

Records are shared electronically.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

Yes

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.11. Does the project place limitation on re-disclosure?

☐ N/A

Yes

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

To request access to information maintained in FOIAXpress relating to a request under FOIA or Privacy Act, individuals can contact the FOIA Requestor Service Center or log in to https://foiaxpress.pal.ed.gov/app/Home.aspx.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

To request access to information maintained in FOIAXpress relating to a request under FOIA or Privacy Act, individuals can contact the FOIA Requestor Service Center or log into https://foiaxpress.pal.ed.gov/app/Home.aspx.

6.3. How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of these procedures on the during the request process and during the creation of a FOIAXpress account.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

FOIAXpress is a major application requiring a system security plan. The system security plan (SSP) details the security requirements and describes the security controls that are in place to meet those requirements. The plan includes the following controls:
• All physical access to the Department site, and the sites of the Department contractors where this system of records is maintained, is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge.
• The computer system employed by the Department offers a high degree of resistance to tampering and circumvention.
• The security system limits data access to the Department and contract staff on a "need to know" basis, and controls individual users ability to access and alter records within the system. Employee and contract staff are only allowed access to the Department's internal network after completing the required annual cybersecurity and privacy awareness training which includes the handling of sensitive PII.
• All users of this system are given a unique user ID with personal identifiers and are required to utilize a complex password.
• All interactions by individual users with the system are recorded.
• Additional strict access controls are in place to ensure each FOIA specialist only sees the records specific to their case or Principal office

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

FOIAXpress is required to be granted an Authorization to Operate (ATO) on a tri-annual basis. This process includes a rigorous assessment of security controls, a plan of action and milestones to remediate any deficiencies, and a continuous monitoring program

between the full scope assessments. Additional actions include monthly scanning, patch deployment, and yearly incident response plan/disaster recovery testing.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner is responsible for all security and privacy documentation as well as ensuring yearly security assessment are performed for the system. Since FOIAXpress is hosted in the cloud, security responsibility will be split between the cloud service provider and the Department but the privacy controls are the sole responsibility of the system owner.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

PII could be inadvertently released if sent to wrong person. To mitigate this risk, the analyst is required to confirm information is correct before records are released.