Privacy Impact Assessment (PIA)
for the
FOIAXpress in the Cloud

This PIA was originally approved on Feb 23, 2018 and reviewed on Feb 23, 2018 by the system owner certifying the information contained here is current and up to date.

Contact Point

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

System Owner

Name/Title: Angela Arrington
Program Office: Office of Management (OM)

Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 N/A Describe the system including the system name, system acronym, and a brief description of the major functions.

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). 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.

FOIAXpress is migrating from its current platform, which is hosted on the EDUCATE network, to the cloud, which is hosted by AINS, Inc.

1.2 N/A Describe the purpose for which the personally identifiable information (PII)\(^1\) is collected, used, maintained or shared.

FOIAXpress collects the names, addresses, dates of request and responses, descriptions or identifications of records requested. The PII from the information collected is used to track, search and respond back to a request or requester.

\(^1\) 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. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf)
1.3 □ N/A Is this a new system, or one that is currently in operation?

Currently Operating System

1.4 □ N/A Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

Updated PIA

Original Publication Date: 01/27/2014

1.5 □ N/A Is the system operated by the agency or by a contractor?

Contractor

2. Legal Authorities and Other Requirements

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

2.1 □ N/A What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?


2.2 □ N/A Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification? Please answer YES or NO.

Yes
2.2.1 □ N/A If the above answer is **YES** this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).

Please provide the SORN name and number, or indicate that a SORN is in progress.

**Freedom of Information Act and Privacy Act Tracking System (18-05-20)**

---

**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 □ N/A Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Records relating to Freedom of Information Act and Privacy Act Tracking System are retained in accordance with General Records Schedule (GRS 14).

- FOIA Requests Files – GRS 14, Item 11a (Ed Schedule No.: 151)
- FOIA Appeals Files – GRS 14, Item 12.a-c (Ed Schedule No.: 152)
- FOIA Control Files –GRS 14, Item 13.a-c (Ed Schedule No.: 153)
- FOIAxpress - ED 086 Information Systems Supporting Materials for System Software

---

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://connected.ed.gov/om/Documents/SORN-Process.pdf)
2.4 □ N/A Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer YES or NO.

Yes

3. Characterization and Use of Information

Collection

3.1 □ N/A List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

FOIAXpress collects the names, addresses, 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 a requester can include name, address, email, phone number, date of birth, Social Security Number (not required for FOIA request), complaint number, and/or loan number.

3.2 □ N/A Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer YES or NO.

Yes

3.3 □ N/A What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.)?

This system includes records and related correspondence on individuals who have submitted: Requests for information under the provisions of the Freedom of Information Act (5 U.S.C. 552), including requests for review of initial denials. Requests under the provisions of the Privacy Act (5 U.S.C. 552a) for records about themselves, including: Requests for notification of the existence of records about them. Requests for access to these records. Requests for amendment of these records. Requests for review of initial denials of such requests for notification, access, and amendment. Requests for an accounting of disclosure of records about them.
3.4 □ N/A  How is the information collected from stated sources (paper form, web page, database, etc.)?

Information collected from the stated sources are received either in paper form, web page, email, database or fax.

3.5 □ N/A  How is this information validated or confirmed?\(^3\)

Privacy Act requests are validated with the information provided by the requester in the certification of identity form.

---

\(^3\) Examples include form filling, account verification, etc.
Use

3.6 □ N/A  Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

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). 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.

3.7 □ N/A  Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

3.7.1 □ N/A  If the above answer is YES, what controls are in place to minimize the risk and protect the data?
3.8 □ N/A Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 □ N/A If the above answer is YES, please explain.

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.*

3.9 □ N/A Does the system collect Social Security Numbers? Please answer YES or NO.

No

3.9.1 □ N/A If the above answer is YES, explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

The Department does not request or require Social Security Numbers (SSNs) and discourages the use of SSNs when submitting requests. However, sometimes requesters will submit SSNs as part of their request. If requester provides SSN in their request, it is redacted in the system.
3.10 ☐ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

4. Notice

4.1 ☐ N/A How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

A notice is provided to users on the “FOIA Request and Appeals” instruction page and the Privacy Act Request instruction page, and is accessible to the public at:


How Information About You is Collected and Shared With Other Organizations

All physical access to the Department site, and the sites of 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. This security system limits data access to Department and contract staff on a "need to know" basis, and controls individual users' ability to access and alter records within the system. All licensed users of this system of records are given a unique user ID with personal identifiers. All interactions by individual users within the system are recorded.

What opportunities are available for individuals to consent to uses, decline to provide information, 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.

5. Information Sharing

Internal

Will information be shared internally with other ED organizations? Please answer YES or NO. If the answer is NO, please skip to Question 5.4.

Yes
5.2 N/A  What information will be shared and with whom?

Information regarding the requester, the request and responsive documents will be shared between the appropriate program offices within the Department in order to fulfill the request.

5.3 N/A  What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

Information regarding the requester, the request and responsive documents will be shared between the appropriate program offices within the Department in order to fulfill the request. This aligns with the stated purpose in Question 1.2.

External

5.4 N/A  Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer YES or NO. If the answer is NO, please skip to Question 5.8.

Yes
Aggregated information in the form of a quarterly report and annual report is submitted to the Department of Justice pursuant to 5 U.S.C. § 552(e)(1).

Additionally, the Department may disclose information contained in a record in this system of records under the applicable routine uses without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected, i.e., tracking FOIA and PA requests. Possible disclosures include:

- Disclosure to Congress, Other Agencies, or the Public
- Disclosure to Recipients of Federal Financial Assistance, Witnesses, or Consultants
- Disclosure for Use by Other Law Enforcement Agencies
- Enforcement Disclosure
- Litigation and Alternative Dispute Resolution (ADR) Disclosures
- Freedom of Information Act Advice Disclosure
- Research Disclosure
- Congressional Member Disclosure

Additional routine use disclosures may be found in the System of Records Notice referenced in Question 2.2.1 above.

The purpose for sharing the information with the organizations above relates to the operation and administration of the FOIA and Privacy Act programs, and compliance with laws and regulations. This aligns with the stated purpose in Question 1.2.
5.7 □ N/A How is the information shared and used by the external entity?

Any disclosures made under the routine uses described above are used by the external entity in accordance with the System of Records Notice referenced in Question 2.2.1 above.

5.8 □ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer YES or NO.

No

5.9 □ N/A Does the project place limitation on re-disclosure? Please answer YES or NO.

No

6. Redress

6.1 □ N/A What are the procedures that allow individuals to access their own information?

The procedures for Redress are found in the System of Records Notice referenced in Question 2.2.1 above.

4 If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.
6.2 □ N/A What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures for the individual to correct inaccurate or erroneous information are found in the System of Records Notice referenced in Question 2.2.1 above.

6.3 □ N/A How does the project notify individuals about the procedures for correcting their information?

The individuals are notified of the procedures for correcting their information in the System of Records Notice referenced in Question 2.2.1 above. Additionally, this information is found at https://www2.ed.gov/policy/gen/leg/foia/foiatoc.html.

7. Safeguards

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

7.1 □ N/A Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer YES or NO.

Yes
What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

FOIXpress is accessible only to Department employees and contractors who work on FOIA and Privacy Act requests and who have a need to know. To access the system, each user must have access to the EDUCATE network. Once logged in the EDUCATE network, the user must have a userid and password to FOIXpress. FOIXpress website is only available internally and is not public facing.

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

The information collected is secured following the guidance contained in OMB Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources,” and P.L. 100-235, “Computer Security Act of 1987.” FOIXpress is a component of the Department’s network, EDUCATE, which 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.
- All users of this system of records are given a unique user ID with personal identifiers.
- All interactions by individual users with the system are recorded.

Is an Authority to Operate (ATO) required? Please answer YES or NO.

Yes

Is the system able to provide account of any disclosures made? Please answer YES or NO.

Yes
7.6 □ N/A  Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.  

Yes

7.7 □ N/A  Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.  

Yes

7.8 □ N/A  Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.  

SSP lists monitoring, testing and evaluation controls for the system. Such activities include monthly scans and yearly incident response plan/disaster recovery testing.

---

8. Auditing and Accountability

8.1 □ N/A  How does the system owner ensure that the information is used in accordance with stated practices in this PIA?  

Yearly security assessment is performed for the system.
PII could be inadvertently released if sent to wrong person. Analyst is required to confirm information is correct before records are released.

Since the FOIAXpress is migrating to the cloud, security responsibility will be split between AINS and the Department of Education (ED). Two entries have been created in CSAM to identify which security controls AINS and ED. ED AINS will be security controls monitored by AINS while FOIAXpress in the Cloud will be monitored by ED.