Privacy Impact Assessment (PIA)
for the

FOIAXpress in the Cloud (FX Cloud)
October 1, 2021

For PIA Certification Updates Only: This PIA was reviewed on **May 13, 2021** by **Arthur Caliguiran** 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/Directory, 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 U.S. Department of Education (the Department) utilizes a commercial off-the-shelf web-based system called FOIAXpress in the Cloud (FX Cloud). 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 U.S. Department of Justice (DOJ), as required by FOIA.

The FX Cloud system processes FOIA request data received by FOIAXpress users. FOIAXpress users are Department FOIA office staff who log in to the system using login/password credentials. FOIA data consist of requests for information received from the public, which includes personally identifiable information (PII), and financial information related to the processing of the FOIA request.

Users utilize FX Cloud for two main purposes:

- Uploading, reviewing, and redacting FOIA and PA documents.
- Running reporting metrics.

The system works through the following process:

- A FOIA or PA request is entered into the FX Cloud system by the Department or can be entered by the requester through the Public Access Link (PAL). Requester will need to create an account in PAL in order to submit requests through the portal at https://foiaxpress.pal.ed.gov/app/Home.aspx
- The request is sent through the system to the Department office(s) that have responsive records.
- If responsive records are found, the Department office(s) will upload those documents into FX Cloud; FX Cloud users will then apply FOIA exemptions if needed.

The response is sent to the requester outside of FX Cloud after the search for responsive records is completed. In addition to processing FOIA requests, the FX Cloud system aids the Office of the Secretary in responding to requests for information concerning the processing and completion of FOIA requests that pertain to all principal offices within

the Department. The requests may come from executive level managers at the Department, principal office chiefs of staff, congressional offices, and FOIA requesters.

FOIAXpress users are Department personnel and contractors, including business and correspondence specialists, subject matter experts, coordinators, and related staff. To create accounts for FOIAXpress users, the system collects name, email address, and program office.

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

FX Cloud collects the names, addresses, dates of request and responses, types of requesters, any correspondence with the requester, and descriptions or identifications of records requested. For Privacy Act requests, the certification of identity (COI) form requests Social Security number (SSN) and date of birth (DOB). SSN and DOB assures that the correct student loan records are retrieved. The other PII from the information collected is used to track, search, and respond back to a request or requester.

FX Cloud also collects name, email address, username, and password from Federal employees and contractors to create their user profiles.

.

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?

Updated PIA

The PIA is being updated as part of the Department's biennial review. During the review process, changes were made to clarify the purpose of the system and the description of its operation.

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

Contractor

[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

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)

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

[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

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 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

2.4. 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.

Department offices provide documents in FOIAXpress that may be responsive to a FOIA or PA request. Those documents will include data about the request, including 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 logs of users accessing the system. Documents responsive to a request can also contain many types of PII present in Department records, such as financial information, loan information, and SSNs or other identification numbers.

Data elements provided by a requester can include name, address, email, phone number, username, password, date of birth, SSN (not required for FOIA request), complaint number, and/or loan number. The same types of information are collected for both FOIA and PA requests. User registration is required for submitting electronic requests for information, and user IDs and passwords are collected as part of the registration process.

The system collects name, email address, username, and password from Federal employees and contractors.

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

Yes

The FX Cloud system collects only that information required to respond to the request, and for users to access the system. No additional information is collected.

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

Department offices provide documents in FOIAXpress that may be responsive to a FOIA or PA request. Those documents will include data about the request, including 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 logs of users accessing the system. Documents responsive to a FOIA request can also contain many types of PII present in Department records, such as financial information, loan information, and SSNs or other identification numbers.

Sources of the information are individuals or third parties who have obtained consent on behalf of the individual.

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 can be collected by mail, through the online FOIA portal, email, or FAX.

Users provide name, address, and phone number as part of the account creation process for making PA or FOIA requests, if submitting their request through the on-line FOIA portal.

When a mailed, emailed, or faxed request is received, the information contained in that request is transcribed into FOIAXpress by ED staff.

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?

PA requests are validated with the information provided by the requester in the COI Certification of identity form when they submit their requests. PA requests are received for student loan records and for investigations regarding alleged civil rights violations only. In order to validate the information, the requester is sent a certification of identity (COI) form. The requester provides for SSN and date of birth DOB on this COI form which is then validated against existing student loan records or records held by the Office for Civil Rights (OCR) as appropriate. A FOIA request does not require validation of the requester.

Use

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

Requesters' PII is used to document, track, and respond to requests made under both FOIA and the PA. Users' PII is used to establish accounts so they may access FX Cloud. PA requests are received for student loan records and for investigations regarding alleged civil rights violations only. In order to validate the information, the requester is sent a COI form. The requester provides the SSN and DOB on the COI form which is then validated against existing student loan records or records held by OCR, as appropriate. The SSN and DOB assures that the correct student loan records or civil rights complaint information are retrieved from the appropriate program office.

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

[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.

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.

3.8. 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

Department offices provide documents in FOIAXpress that may be responsive to a FOIA request. Those documents will include data about the request, including 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 logs of users accessing the system. Documents responsive to a FOIA request can also contain many types of PII present in Department records, such as financial information, loan information, and SSNs or other identification numbers.

Data elements provided by a requester can include name, address, email, phone number, DOB, SSN (not required for FOIA request), complaint number, and/or loan number. The same types of information are collected for both FOIA and PA requests.

In order to process a PA request, the requester is required to submit a COI form. The COI form requests for SSN and DOB. The SSN and DOB assures that the correct student loan records or civil rights complaint information are retrieved from the program office. However, sometimes requesters will submit their SSNs in their request description. If requester provides an SSN in a request, the SSN is removed from the description field in the FOIAXpress case since FOIA logs include the request description.

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

☑ N/A

Click here to enter text.

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.

A notice is provided to users on the bottom of "FOIA Request and Appeals" forms and the Privacy Act Request form, and is accessible to the public to download at:

http://www.ed.gov/policy/gen/leg/foia/request_foia.html
http://www.ed.gov/policy/gen/leg/foia/request_privacy.html

A notice is provided to requesters on the PAL portal on the bottom of the request form.

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

Privacy notice provided to requesters on bottom of FOIA request form and appeal form:

Privacy Act Statement:

AUTHORITY: 5 U.S.C. 301, Departmental Regulations and 5 U.S.C. 552, Freedom of Information Act (FOIA).

PURPOSE: to allow individuals to file electronic FOIA requests; to track all FOIA requests from receipt to response to compile statistics for the Annual FOIA Report; to research and respond to FOIA requests; to maintain case files to comply with records disposal requirements; and to maintain an administrative record to support any litigation.

ROUTINE USE: Requests are received, assigned a case number, routed to the appropriate office or organization for research and response, and filed in a case file. Requests that are transferred, receive a no records response, or granted in full are retained for 2 years and then destroyed. Requests that are denied in whole or in part are retained for 6 years then destroyed.

DISCLOSURE: Voluntary. We seek your full name and postal mailing address so we may mail a response to you. Failure to provide this information may result in your request not being processed (this page does not capture email addresses).

Information collected by this form is also used for trend analysis and may be shared with law enforcement personnel. Information submitted may be retained indefinitely.

Privacy notice provided to requesters on bottom of Privacy Act form:

Privacy Act Statement.

In accordance with 34 CFR Section 5b.5(b)(2) personal data sufficient to identify the individuals submitting requests by mail under the Privacy Act of 1974, 5 U.S.C. Section 552a, is required. The purpose of this solicitation is to ensure that the records of individuals who are the subject of U.S. Department of Education systems of records are not wrongfully disclosed by the Department. Requests will not be processed if this information is not furnished. False information on this form may subject the requester to criminal penalties under 18 U.S.C. Section 1001 and/or 5 U.S.C. Section 552a(i)(3).

Privacy notice provided to requesters on PAL on bottom of request form:

Privacy Act Statement. In accordance with 34 CFR Section 5b.5(b)(2) personal data sufficient to identify the individuals submitting requests by mail under the Privacy Act of 1974, 5 U.S.C. Section 552a, is required. The purpose of this solicitation is to ensure that the records of individuals who are the subject of U.S. Department of Education systems of records are not wrongfully disclosed by the Department. Requests will not be processed if this information is not furnished. False information on this form may subject the requester to criminal penalties under 18 U.S.C. Section 1001 and/or 5 U.S.C. Section 552a(i)(3).

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid OMB control number. The valid OMB control number for this information collection is 1880-XXXX. Public reporting burden for this collection of information is estimated to average 0.50 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Obligation to respond is voluntary. If you have questions on your individual submission of this form, write directly to: FOIA Service Center, U.S. Department of Education, 400 Maryland Avenue, S.W., 7W104, Washington, D.C. 20202-4537.

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 requesters do not want to provide any of the required information, they can decline to provide it. 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.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

Information regarding the requester, the request, and responsive documents are shared with the appropriate program offices.

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

☐ N/A

Information regarding the requester, the request, and responsive documents are shared to fulfill the request.

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.

No

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

Click here to enter text.

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

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

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

☑ N/A

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

☑ N/A

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

[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

6. Redress

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

Requesters creating accounts in FOIAXpress have no access to their submitted information.

If an individual wishes to gain access to a record they have requested through a Privacy Act request, he or she should contact the system manager at the appropriate office or region where the original PA requests were sent, or from where the response was received. A request to amend a record must meet the requirements of the Department's PA regulations in 34 CFR 5b.5, including proof of identity.

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

Requesters creating accounts in FOIAXpress have no access to their submitted information.

The procedures for the individual to correct inaccurate or erroneous information are found in the system of records notice. If an individual wishes to gain access to a record in this system of records, he or she should contact the system manager at the appropriate office or region where the original FOIA or PA requests were sent, or from where the response was received. A request to amend a record must meet the requirements of the Department's PA regulations in 34 CFR 5b.5, including proof of identity.

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

Notification of individuals regarding the procedures for correcting information are found on the privacy notice at the point of collection, as well as in this PIA and the SORN.

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?

FX Cloud is a secure, online system, has had extensive security testing and meets all security requirements for a moderate-level system. The information is secured according to the requirements found in all applicable Department policy. The system complies with IT security requirements in the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) circulars, and the National Institute of Standards and Technology (NIST) standards and guidelines. FX Cloud is monitored continuously by the Information System Owner (ISO) and the Information System Security Officer (ISSO), as well as the contractor operating the system. Vulnerabilities are identified, documented, and resolved in accordance with Federal requirements. Electronic information is secured using access controls, background clearances, personnel security awareness and training, and regular auditing of information and information management processes. All users are properly identified and authorized for access, are made aware of the rules, and agree to abide by them as stated. In addition, security is maintained through carefully managed control of system changes, appropriate contingency planning, handling, and testing, and by ensuring that any incident is handled expeditiously.

Account access within the system is also limited in that users have a defined time during which their access is actually active. This automatic feature will log out inactive users and disable their user account based on their access needs. The system can generate both usage and customized access reports that will report users who have been inactive or disabled from the system as needed.

To access FX Cloud, users must receive approval from their program office and the program office FOIA Coordinator will request a user license from the FOIA Service Center. The FOIA Service Center will determine if user license request is approved.

Additionally, the audit trail feature, unique identification, authentication and password requirements, and mandatory security, privacy and records training requirements help prevent unauthorized access to data, browsing and misuse.

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.

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

A yearly security assessment is performed for the system. During the assessment, random controls are tested to ensure Department security protocols are adhered to.

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?

The main privacy risk identified is unauthorized access to the PII contained in FX Cloud. This PIA details the privacy controls and safeguards implemented for this system to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. Additionally, privacy risks have been reduced by only collecting the minimum PII necessary to process the request.

Risk has been further mitigated through privacy training for both contractors and Department staff, restricting access to PII to those individuals with a direct business need for the information, working closely with Department security and privacy staff, and robust security controls such as the use of firewalls, intrusion detection systems, and event monitoring systems.

In most cases in a FOIA request, there is minimal harm to the agency or the individual if privacy related data is disclosed, intentionally or unintentionally, because the PII in the system is not considered sensitive (i.e., name, work phone number, email). However, in a PA request, because the PII is sensitive (name, address, phone number, email, SSN, and DOB), the individual's identity could be compromised and result in identify theft or financial loss. As stated in question 7.4, there are multiple layers of technical and administrative safeguards in place to mitigate the risks inherent with unauthorized disclosure.

Privacy Impact Assessment (PIA) Signature Page