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

November 9, 2023

Point of Contact

Contact Person: Art C. Caliguiran
Title: Director of Privacy and Appeals
Email: arthur.caliguiran@ed.gov

System Owner

Name: Art C. Caliguiran
Title: Director of Privacy and Appeals
Principal Office: Office of the Secretary (OS)

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

Please complete this ***Privacy Impact Assessment (PIA)****, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The U.S. Department of Education (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 annual and quarterly reports to the U.S. Department of Justice (DOJ), as required by FOIA.

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

FX Cloud users utilize FX Cloud for two main purposes:

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

FX Cloud processes FOIA request data received by Department FOIA office staff who log in to the system using their PIV card. FOIA request data consists of requests for information received from the public, which includes personally identifiable information (PII) and financial information (payment from the FOIA requester, if applicable) related to the processing of the FOIA request.

For external users, the Department uses the FOIAXpress Public Access Link (PAL) module, a secure public-facing web portal that is integrated with the General Services Administration’s Login.gov to provide a single access point for requesters to create individual accounts, submit requests, access requested records, and communicate with the Department about the status of a request.

The Department connects with Login.gov to allow ongoing authentication services for external users submitting a FOIA or PA request using the PAL module. Individuals creating an account with PAL are redirected to Login.gov for ID verification and authentication in conformance with the National Institute of Standards and Technology's (NIST) Digital Identity Guidelines (Special Publication 800-63-3). Users are required to agree to Login.gov's Rules of Use prior to using the service.

The Department has defined the attributes to be shared with Login.gov during the process of onboarding Login.gov with FX Cloud. The list of attributes can be found here (FX Cloud collects information under the "ID Proofed" column). PII collected, stored, protected, shared, and managed electronically by Login.gov is out of scope of this PIA.

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 PAL. The requester will need to create an account in PAL and authenticate through Login.gov 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.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

FX Cloud 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 PAL. The requester will need to create an account in PAL and authenticate through Login.gov 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 FX Cloud system data include:

- Tracking number.
- Requester PII (see question 3 for further details).
- Date of the request.
- Department office designated for response.
- FOIA exemption codes – redacted portions of records will be labeled if FOIA exemptions are applied. FOIA exemption codes are not included in source documents but are applied by FOIA analysts within the system.
- The system can collect any information that is part of a FOIA request. Examples of PII include but are not limited to, complaint numbers, Social Security numbers (SSNs), financial data, and grant numbers.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☐ Application
☒ Database	☐ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

PII is collected and processed for (1) creating accounts for access to FX Cloud for FOIA and PA requesters, (2) responding to FOIA or PA requests, and (3)documenting and tracking the status of requests made under both the FOIA and PA. In addition, PII is collected and maintained to create Department FX Cloud user and administrator accounts.

[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. Is the IT system operated by the agency or by a contractor?

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

The Department manages FX Cloud for the day-to-day activities of the application. The vendor hosts the application in the cloud and addresses technical issues escalated by Department staff.

□ N/A

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

Yes

□ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each 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 (Public Law 110–81, 121 Stat. 735); the Privacy Act of 1974, 5 U.S.C. 552a, as amended; the Foundations for Evidence-Based Policymaking Act of 2018 (Public Law 115–435, 132 Stat. 5529) and Departmental Regulations, 5 U.S.C. 301.

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

The SORN, titled "Freedom of Information Act and Privacy Act Tracking System," 18-05-20, 80 FR 30671, was published in the Federal Register on May 29, 2015.

Records Management

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

Records relating to the FOIA and PA 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.

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☒ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☒ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☒ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☐ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☐ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☒ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver’s License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☒ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☒ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☒ Student Loan Number	☒ Grant Number
☒ Other ID That Can Be Traced to Individual (Specify below) UUID		

Electronic and Miscellaneous Information

☒ Username/User ID	☐ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals

☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to “specify below,” describe the PII:

In addition, any information contained in responses to FOIA and PA requests will also be maintained on the system.

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:

Name, work email address, program office, and username are required to create accounts for FX Cloud users and system administrators.

Any information contained in responses to FOIA and PA requests will also be maintained on the system.

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Name, work email address, program office, and username are required to create accounts for FX Cloud users and system administrators.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each.

From FOIA and PA requesters: name, email address, requester category (*i.e.,* whether a requester is making a FOIA request or a PA request), and username are required to create an account for requesters in PAL. NOTE:

For PA requests, third-parties representing an individual with their consent, can submit a PA request on the individual's behalf.

For FOIA requesters: name, address, email address, date of request, type of requester, any correspondence with the requester, and descriptions or identifications of records requested. In addition, the amount of fees paid, if any; payment delinquencies, if any; final determinations of appeals or denials; and logs of the requester accessing the system. The system can also collect any information that may be subject to disclosure pursuant to a FOIA request. Examples include but are not limited to, complaint numbers, SSNs, financial data, and grant numbers.

For PA requesters: certification of identity (COI) form, which includes the requester's SSN and DOB. Collecting the SSN and DOB helps the Department to assure that the correct records are retrieved. Name, mailing address, email address, and phone number are collected to track, search, and respond back to a request or requester.

Any other information contained in responses to FOIA and PA requests will also be maintained on the system.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

Sources of the information are persons who are making a FOIA or PA request, or third parties who have obtained consent on behalf of an individual to submit a PA request. Department offices provide documents in FX Cloud that may be responsive to a FOIA or PA request. Documents responsive to a FOIA request can contain many types of PII present in Department records, such as financial information, loan information, and SSNs or other identification numbers. Documents responsive to a PA request 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.

For Department administration and use of the system, sources of PII are Department employees and contractors.

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

Information can be collected by mail, through the online FOIA portal, or by email or fax. Requesters provide their name, address, and phone number as part of the account creation process for making PA or FOIA requests if submitting their request through the online FOIA portal. When a mailed, emailed, or faxed request is received, the information contained in that request is transcribed into FX Cloud by Department staff.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

PII provided by a requester can include name, address, email, phone number, DOB (not required for FOIA request), SSN (not required for FOIA request), complaint number, and/or loan number. This information is necessary to properly research and respond to 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 ensure that the correct records (*e.g.,* student loan records or civil rights complaint information) are retrieved from the program office. Department offices provide documents in FX Cloud that may be responsive to a FOIA request.

In order to process a FOIA request, the requester is required to submit information that will allow the Department to properly research and respond to a request. This includes contact information (*e.g.,* name, email address). Department offices provide documents in FX Cloud that may be responsive to a FOIA request. In addition to the responsive documents, the Department will also provide 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 contain many types of PII present in Department records, such as financial information, loan information, and SSNs or other identification numbers. This information is needed in order for the Department to review and redact the potentially responsive records, as well as to provide the records to the requester.

However, sometimes FOIA requesters will erroneously submit their SSNs in their request description. If a FOIA requester provides an SSN in a request, the SSN is removed from the description field in the FX Cloud case since FOIA logs include the request description.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☒ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

PA requests are validated with internal Department records from the information provided by the requester in the COI form when they submit their requests.

The requester provides for SSN and DOB on this COI form which is then validated against the records being sought by the requester (*e.g.,* existing student loan records or records held by the Office for Civil Rights. A FOIA request does not require validation of the requester. The records that are responsive to a PA or FOIA request are taken from other Department systems and validated within those other systems.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ N/A

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. Does the IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.9.1. If the above answer to question 3.10 is **YES**, cite the authority for collecting or maintaining the SSNs.

□ N/A

The collection of SSNs of PA requesters that are maintained in this system is authorized by 5 U.S.C. 301 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

3.10.2. If the above answer to question 3.10 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

□ N/A

To process a PA request, the requester is required to submit a COI form. The COI form collects the requester's SSN and DOB. The SSN and DOB help the Department ensure that the correct records are retrieved from the program office and help prevent an improper disclosure.

3.10.3. If the above answer to question 3.10 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

□ N/A

For PA requests, the COI form requests SSN and DOB, which both are mandatory fields.

3.10.4. If the above answer to question 3.10 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

□ N/A

Alternatives to SSNs were considered but were determined to not be feasible. The Department has an obligation to ensure that we are only providing records to a PA requester that the requester is authorized to obtain under the statute. Because of the records maintained by the Department, there is not an alternative to the SSN that would allow the Department to perform this function and ensure that the correct records are retrieved from the respective program office and provided to the requester.

Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

A PA statement is located at the bottom of the FOIA Request form, FOIA Appeals form, and the Privacy Act Request form. See the links below to gain access to the forms.

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

A PA statement is also provided to requesters on the FX Cloud portal at the bottom of the request form.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

N/A

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

A PA statement is provided to requesters at the bottom of the FOIA Request and FOIA appeal forms and online through the FX Cloud portal when submitting a FOIA request and/or appeal:

> **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.

A PA statement is provided to requesters at the bottom of the Privacy Act Request form and online through the FX Cloud portal when submitting a PA request:

> **Authorities**: The information requested on this form, and the associated evidence, is collected under the Privacy Act of 1974 (Privacy Act), 5 U.S.C. Section 552a, as amended.
>
> **Purpose**: The primary purpose for providing the requested information on this form is to request access to information under the Privacy Act, or amendment or correction of records under the Privacy Act. The Department uses the information you provide to (1) identify your identity, and (2) grant or deny the information request you are seeking or requesting to amend.
>
> **Consequences of Failure to Provide Information**: The information you provide is voluntary. However, failure to provide the requested information, and any requested evidence, may delay access to information or result in denial of your information or amendment request.
>
> **Routine Uses**: The Department may share the information you provide on this form and any additional requested evidence in accordance with disclosures permitted under 5 U.S.C. 552a(b) of the Privacy Act. In addition, information contained in this system may be disclosed outside of ED as a routine use pursuant to 5 U.S.C. 55a(b)(3) when the disclosure is compatible with the purpose for which the records were compiled. The routine use disclosures are detailed in the

system of records titled “Freedom of Information Act and Privacy Act Tracking System” system of records notice, located on the Department’s system of records notice website.

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Requesters may freely decline to provide any information they do not wish to provide; however, such a refusal may adversely affect the Department’s ability to process a FOIA request, appeal, or PA request if the submitted information is inadequate or the individual’s identity cannot be authenticated (for a PA request).

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

□ 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 each Department IT system(s) and/or principal office specified in Question 5.2?

□ N/A

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

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

□ N/A

Depending on the type of request (FOIA, PA), different categories of PII may be shared with the requester. For FOIA requests, the Department will review and redact the potentially responsive records, and provide the records to the requester.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

□ N/A

The purpose of sharing PII is to fulfill the request made under the provisions of the FOIA and PA.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

□ N/A

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 (Public Law 110–81, 121 Stat. 735); the Privacy Act of 1974, 5 U.S.C. 552a, as amended; the Foundations for Evidence-Based Policymaking Act of 2018 (Public Law 115–435, 132 Stat. 5529) and Departmental Regulations, 5 U.S.C. 301.

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

□ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

□ N/A

Responsive records could be shared with requesters within the FX Cloud system, by email, or through paper correspondence.

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

□ N/A

No

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

□ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

Requesters who submit a PA request can access the responsive records in FX Cloud.

In addition, 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.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

If an individual wishes to contest the content of a record pertaining to him or herself that is contained in the 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 (see appendix), 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.7.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

Notification to individuals regarding the procedures for correcting information is found on the PA statement at the point of collection, as well as in this PIA and the SORN, referenced above in question 2.3.

7. Safeguards

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

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate

☐High

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

FX Cloud is a secure, online system that has had extensive security testing and meets all security requirements for a moderate-level system. 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. PII in FX Cloud is secured by implementing NIST Special Publication 800-53 compliant security controls including strong encryption, secure passwords, two-factor authentication (2FA), requiring data in transit TLS encryption, using secure encrypted wireless and virtual private networks (VPNs), and requiring that data at rest be encrypted. All decommissioned media are properly sanitized before disposal. FX Cloud is monitored continuously by security vulnerability scanners to detect intrusions and prevent data breaches. In addition, FX Cloud is continuously patched to ensure it has the latest security updates.

All users are properly identified and authorized for access, are made aware of the rules, and agree to abide by them as stated. Account access within the system is also limited in that users have a defined time during which their access is active. This automatic feature will log out inactive users. 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.
In addition, security is maintained through carefully managed control of system changes, appropriate contingency planning, handling, and testing to assist in preventing unauthorized access to data, unauthorized browsing, and misuse.

Through the integration with Login.gov, all external users, those making FOIA or PA requests, are required to use multifactor authentication to access FX Cloud.

8. Auditing and Accountability

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

The information system owner (ISO) works with the Department's Privacy Program to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document. In addition, all FX Cloud users sign a user agreement that indicates the proper use of the data and the consequences of not following the rules of behavior. User accounts are reviewed annually to ensure only authorized users have access.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

FX Cloud is monitored continuously by the ISO and the Information System Security Officer (ISSO), as well as the contractor operating the system.

The system administrator runs required scans/tests on a monthly and annual basis as required. Security and system documentation is updated as required. Monitoring and auditing of all event logs are performed on a regular basis. Patches are checked for, tested, and applied to the server weekly, depending on necessity. When going through the ATO/Ongoing Security Authorization (OSA) process, the system owner establishes monitoring processes to ensure the information is used in accordance with the approved practices. During the OSA process, smaller subsets of security controls are tested every quarter.

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

Privacy risks associated with FX Cloud include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs. The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.