U.S. Securities and Exchange Commission

Electronic Freedom of Information Act Processing System (eFOIA)

PRIVACY IMPACT ASSESSMENT (PIA)

June 30, 2021

Office of Support Operations

Privacy Impact Assessment

eFOIA

Section I: System Overview

1.1 Name of Project or System

Electronic Freedom of Information Act Processing System (eFOIA)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC)

☐ Externally hosted (Contractor or other agency/organization):

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed: 5/7/2002

Last updated: 1/29/2016

Description of update: Continuous monitoring updates to reflect current version of the system (v10.2) and to move information to current PIA Template.

1.4 Does the system or program employ any of the following technologies?

☐ Electronic Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☐ Cloud Computing Services

☐ www.sec.gov Web Portal

☒ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

The eFOIA system is used by the Office of FOIA Services (OFS) to track and process Freedom of Information Act (FOIA), Privacy Act (PA), and SEC Rule 83 (Confidential Treatment Procedure) requests. A typical transaction may consist of a request from the public for non-public records under the FOIA, for public information which has not been published to the SEC Website under the FOIA, (i.e., paper registration filings and other routine releases of the Commission prior to 1996), or requests under the PA. OFS will release records to a requester to the extent that information within the records is not subject to exemption or exclusion.

The eFOIA system consists of two components: FOIAXpress (FX) and Public Access Link (PAL). FX is a suite of commercial off the shelf (COTS) products developed by AINS Inc. to electronically track and manage FOIA and PA requests. FX is used by SEC staff to electronically create, store, retrieve, redact, and print documents for delivery to FOIA requesters. It also keeps track of FOIA processing statistics and fees, and generates reports on the number, types, and nature of FOIA requests processed, as required by the US Department of Justice.

PAL allows requesters, who have submitted FOIA requests, to track their submissions online and allows other interested parties to check the status of pending requests. Two types of users will be able to access PAL. The first type of users are individuals who have previously submitted a request and are seeking a status on that request. These individuals will log in using the same username and password created when they registered their account in PAL. The second type of users are individuals who have not previously registered in PAL, but are interested in the status of any FOIA request. In order to view the status, these users will need to input a FOIA case number. Once this information is entered, the second user will be able to view limited information regarding the FOIA request including: (1) the current status of the FOIA request (i.e. pending, in process, etc.); (2) the FOIA control number; and (3) the date the FOIA request was received by the SEC.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

Freedom of Information Act (FOIA) (5 U.S.C. §552) and the Privacy Act (PA) (5 U.S.C. §552a); Executive Order 9397; SEC Rule 83 (Confidential Treatment Procedure).

2.3 Does the project use or collect Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No
☐ Yes

If yes, provide the purpose of collection:
If yes, provide the legal authority:

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No
☐ Yes, a SORN is in progress
☒ Yes, there is an existing SORN

SEC-11 ("Freedom of Information and Privacy Act Requests")

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☒ No
☐ Yes

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The purpose of this collection is to enable OFS to track and process record requests and appeals under the Freedom of Information Act, access, notification, and amendment requests and appeals under the Privacy Act, and confidential treatment requests under SEC Rule 83 (Confidential Treatment Procedure). A privacy risk is that information provided for one purpose may be used inappropriately for another purpose. This risk is low, as information is not collected without a clear purpose or legal authority. The System of Records Notice (SORN) SEC-11, identified in Section 2.4 above, states the intended and authorized purpose for the data collection.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☐ Social Security Number	☐ Alien Registration	☐ Financial Accounts
☐ Taxpayer ID	☐ Driver's License Number	☐ Financial Transactions
☐ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☒ File/Case ID	☐ Credit Card Number	☐ Employer ID
☐ Other:		

General Personal Data

☒ Name	☐ Date of Birth	☐ Marriage Records
☐ Maiden Name	☐ Place of Birth	☐ Financial Information
☐ Alias	☒ Home Address	☐ Medical Information
☐ Gender	☒ Telephone Number	☐ Military Service
☐ Age	☒ Email Address	☐ Mother's Maiden Name
☐ Race/Ethnicity	☐ Education Records	☐ Health Plan Numbers
☐ Civil or Criminal History	☒ Zip Code	
☐ Other:		

Work-Related Data

☐ Occupation	☐ Telephone Number	☐ Salary
☐ Job Title	☐ Email Address	☐ Work History
☐ Work Address	☐ Certificate/License Number	☐ Business Associates
☐ PIV Card Information	☐ Fax Number	
☐ Other:		

Distinguishing Features/Biometrics

☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording/Signature	☐ Video Recordings	
☐ Other:		

System Administration/Audit Data

☒ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☐ Queries Run	☐ Contents of Files

☒ Other: Failed login attempts, Password changes, & Use of administrative privileges

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

When individuals provide information to the SEC for FOIA and/or PA requests, the SEC uses this information to efficiently and accurately process record requests and administrative appeals under the FOIA and PA, as well as access, notification, and amendment requests and appeals under the PA. Also, the SEC uses such information when defending itself in litigation arising from such requests and appeals; and in assisting the SEC in carrying out any other responsibilities under the FOIA or PA including reporting requirements, such as the Annual FOIA Report.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees
Purpose: Information retrieved in response to a FOIA and/or PA request.

☒ SEC Federal Contractors
Purpose: Information retrieved in response to a FOIA and/or PA request.

☐ Interns
Purpose:

☒ Members of the Public
Purpose: When submitting information to the SEC for FOIA and/or PA requests

☐ Employee Family Members
Purpose:

☐ Former Employees
Purpose:

☐ Job Applicants
Purpose:

☐ Vendors
Purpose:

☐ Other:
Purpose:

3.4 What mechanisms are in place to minimize the use of PII for testing, training, and research efforts?

PII is not used for testing, training, and/or research efforts.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☐ No.

☒ Yes.
eFOIA follows GRS 4.2, Item 020 disposition authority. The records are temporary; Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use; Requests for confidential treatment are retained for 10 years, unless renewed.

3.6 What are the procedures for identification and disposition at the end of the retention period?

FOIAXpress has a file retention policy built into the application. Management team can produce a report that provides all documents that fall into the retention period. Retention policy is active currently.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A
☐ Members of the Public
Purpose:
☐ Employees
Purpose:
☐ Contractors
Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The primary privacy risks relating to the type of information collected are risk of unnecessary or excessive collection of information and inadvertent or unauthorized disclosure of non-public information. To mitigate these risks, request applicants are only required to provide basic contact information and need only provide information in boxes marked with red asterisks. FOIAXpress has a file retention policy built into the application. In addition, all data entered into FX is stored within the SEC network. SEC has implemented strict access control measures for authorized users, has implemented record level security to protect designated case files as well as an automatic timeout feature to prevent unauthorized browsing of the information contained within the FOIA tracking system.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☒ Privacy Act Statement
PAL Requester Registration Form (https://efoia-pal.sec.gov/app/CreateRequester.aspx)
☒ System of Records Notice
SEC-11 ("Freedom of Information and Privacy Act Requests")
☒ Privacy Impact Assessment
Date of Last Update: 1/29/2016
☒ Web Privacy Policy
SEC FOIA page (https://www.sec.gov/about/privacy/secprivacyoffice.htm)
☐ Other notice:

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were these risks mitigated?

There are no identifiable risks associated with openness and transparency. No mitigation actions are recommended. Individuals receive a Privacy Act Statement when they register for a PAL account to track FOIA requests. This PIA and the associated SORN, Freedom of Information Act and Privacy Act Requests, provide constructive notice of the SEC's information collection practices. The SEC notifies the public, including FOIA/PA requesters, and FOIAXpress system users, about what information is collected in the system, and how it is used and disclosed, through applicable system of records notices that the SEC publishes in the Federal

Register and posted online. The SEC's website also contains information on FOIA and the Privacy Act at https://www.sec.gov/page/office-foia-services.

Section 5: Limits on Uses and Sharing of Information

5.1 What types of methods are used to analyze the data?

Data collected in eFOIA is not analyzed.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: Data will be shared with internal organizations. Internally, requests are referred to FOIA liaisons in SEC Divisions and Offices to provide responsive records; SEC Office of Information Technology (OIT) staff and contract support staff have access to the data in order to provide system administration and support.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

The privacy risk associated with internal sharing is inadvertent or unauthorized disclosure of information to individuals without authorization. To mitigate this risk, all authorized SEC users who have access to data in the system must have the approval of the FOIA Program Manager before access is granted to the system. Additionally, the system's functional security limits a user's access to specific functions and regulates a user's ability to update data for a specific function. All access granted is determined on a "need to know" basis. In addition, SEC has implemented strict access control measures for authorized users, has implemented record level security to protect designated case files and an automatic timeout feature to prevent unauthorized browsing of the information contained within the FOIA tracking system.

5.4 Will external organizations have access to the data?

☒ No
☐ Yes

Organizations:

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

The privacy risk from external sharing is unauthorized disclosure. This risk is mitigated by making external disclosures only in accordance with SEC SORN SEC-11. In addition, data transmitted electronically is secured by encryption.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☒ Directly from the individual.
☐ Other source(s):

6.2 What methods will be used to collect the data?

Members of the public and SEC employees and contractors may file FOIA and Privacy Act requests with SEC by mail, fax, email, Webform or online via the PAL request form. PAL allows requesters, who have submitted FOIA requests, to track their submissions online and allow other interested parties to check the status of pending requests.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

Individuals submitting requests are responsible for ensuring that the information they submit is accurate. SEC FOIA liaisons review potentially responsive records and confirm that the information in the records match the information requested.

6.4 Does the project or system process, or access, PII in any other SEC system?

☒ No
☐ Yes.
System(s):

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity. How are these risks mitigated?

There is a potential risk associated with data quality and integrity because requester information may be manually entered into the system by SEC staff. This risk is mitigated as requester information is collected directly from the requesters to the greatest extent practicable. Specifically, the PAL component of the system allows users to enter their requests and contact information directly into the system, and they have the ability to update their information at any time, thereby helping to enhance the accuracy and timeliness of their information. In addition, as a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed prior to releasing records to the requester. Further, the system has built-in data integrity checks to ensure that certain fields are correctly populated.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

When information is collected directly from the individual, the SEC Privacy Program ensures that Privacy Act (e)(3) statements and other privacy notices are provided, as necessary, to individuals prior to the collection of PII. This implied consent from individuals authorizes the collection of the information provided. Additionally, this PIA and the SORN(s) listed in 2.4 serve as notice of the information collection.

7.2 What procedures will allow individuals to access their information?

Persons wishing to obtain information on the procedures for gaining access to the contents of records may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736.

7.3 Can individuals amend information about themselves in the system? If so, how?

Persons wishing to amend information about themselves in the system may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736.

7.4 Discuss the privacy risks related to individual participation and redress. How were these risks mitigated?

There are no identifiable risks associated with access and amendment for FOIA. No mitigation actions are recommended.

Section 8: Security

8.1 Does the project or system involve online collection of personal data?

☐ No
☒ Yes
Public URL: https://efoia-pal.sec.gov/

8.2 Does the site have a posted privacy notice?

☐ No
☒ Yes - https://efoia-pal.sec.gov/app/CreateRequester.aspx
☐ N/A

8.3 Does the project or system use web measurement and/or customization technologies?

☒ No
eFOIA does not use third party web measurement and/or customization technologies to measure and customize the user's experience.
☐ Yes but they do not collect PII
☐ Yes and they collect PII

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system or project.

All SEC staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII.

9.2 Does the system generate reports that contain information on individuals?

☒ No
☐ Yes

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☐ No
☐ Yes
☒ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes
Splunk is currently monitoring FOIAXpress error logs. Error logs e:/Program Files (x86)\AINS FOIAXpress\Logs\FOIAXpress\ErrorLog*.txt and monitoring the server logs. The error log will pick up

application errors and the Server logs will pick up updates, and event logs. Audit trails are also found in FOIAXpress where you can look at failed login attempts, password changes, time in software, as well as what he/she does in the application. The eFOIA Team produces an audit report semi-annually called the User Access Review that is also reviewed by the SEC OIT Security program. Audit logs are retained in consistency with the SEC records retention policy.

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Residual risk related to access can include the inadvertent handling or misuse of data. To minimize this risk, authentication to eFOIA is achieved via SSO (once a user has authenticated to the SEC network) and system privileges (including access to information) are granted based on defined roles.