U.S. Securities and Exchange Commission

Electronic Freedom of Information Act Processing System (eFOIA)
PRIVACY IMPACT ASSESSMENT (PIA)

January 29, 2016

Office Office of Support Operations (OSO), FOIA Services

Privacy Impact Assessment

Electronic Freedom of Information Act Processing System (eFOIA)

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	5/2/06	Document Creation-FOIAXpress
Document update	1	9/9/13	Recertification of FOIAXpress
Document update	2	1/15/16	Integration of Public Access Link (PAL)
Document update	3		
Document update	4		
Document update	5		
Document update	6		

General Information

1. Name of Project or System.
   Electronic Freedom of Information Act Processing System (eFOIA).

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

   The Office of FOIA Services (OFS) is responsible for receiving and responding to requests for non-public records under the Freedom of Information Act (FOIA) (5 U.S.C. §552) and the Privacy Act (PA) (5 U.S.C. §552a) and to requests 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. OFS will release all or portions of requested records to a requester if exempt information can reasonably be removed or deleted and the record is not subject to a FOIA exclusion. OFS utilizes the eFOIA system to track and process FOIA requests.

   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 allows 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 is a new capability added to eFOIA. 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. Two types of users will be able to access PAL. The first type of users is individuals who have previously submitted a request through FX and are seeking a status of that request. These individuals will log in using the same username and password created when they submitted their initial FOIA request. The second type of users is individuals who have not previously submitted a FOIA request, but are interested in the status of someone else's request. In order to view the status, these users will need to input a FOIA case number. Once this information is input, 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.

3. Requested Operational Date? The FX component has been operational since November 2004. The most recent recertification for the system was May 2013. The eFOIA PIA dated September 9, 2013 is being updated to assess the privacy risks introduced by the system's implementation of the PAL component. The PAL component is scheduled to become operational in the fall of 2016.

4. System of Records Notice (SORN) number? SEC-24, Freedom of Information and Privacy Act Requests.

5. Is this an Exhibit 300 project or system? ☒ No ☐ Yes

6. What specific legal authorities, arrangements, and/or agreements allow the collection of this information? 5 U.S.C. §552, as amended and §552a.

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?

   The eFOIA system may collect any personally identifiable information (PII) contained in requests made pursuant to the FOIA, the PA, and SEC Rule 83 (17 CFR 200.83), including, but not limited to, personal information retrieved in response to a request including requesters' and their attorneys' or representatives' names, addresses, e-mail, telephone numbers, and FOIA and PA case numbers; office telephone numbers of SEC employees and contractors; names, telephone numbers, and addresses of the submitter of the information requested; unique case identifier; social security number; or other identifier assigned to the request or appeal; personal information required for location of PA records; internal memoranda; correspondence to or from other federal agencies; correspondence and response letters; appeals of denial under the FOIA; requests for amendment under the PA; appeal for denials under the PA; FOIA and PA appeal determinations and remands; requests for confidential treatment substantiation; appeals of denials of substantiation; determinations and remands; billing invoices; court orders; electronic research; and all types of agency records which may be responsive to a FOIA request. There is no change in the data collected, generated, or retained by the implementation of PAL.

2. Does the project/system use or collect the social security number (SSN)? (This includes truncated SSNs)
   ☒ No.
   ☐ Yes. If yes, provide the function of the SSN and the legal authority to collect.
   However, the SSN may be voluntarily provided as part of requests made pursuant to the FOIA, the PA, and SEC Rule 83 (17 CFR 200.83). In these instances, the SSN is redacted.

3. What are the sources of the data?
   Information is provided to the SEC by: persons requesting confidential treatment from the Commission pursuant to the FOIA, the PA, or SEC Regulation 17 CFR 200.83; individuals who submit FOIA and/or PA requests; individuals who appeal SECs' denial of their FOIA and/or PA requests; individuals whose requests, appeals, and/or records have been referred to SEC by other agencies; attorneys or other persons representing individuals submitting such requests and appeals; individuals who are the subjects of such requests; Department of Justice (DOJ) and other government litigators; and/or SEC personnel assigned to handle such requests or appeals. Additionally information may be retrieved from SEC records that pertain to the information being requested.

4. Why is the data being collected?
   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 SEC in carrying out any other responsibilities under the FOIA or PA including reporting requirements, such as the Annual FOIA Report.

5. What technologies will be used to collect the data?
   Currently requests are mailed, e-mailed or faxed to the FOIA/PA Office. The implementation of PAL will establish a web application that allows users to track requests.

SECTION II - Attributes of the Data (use and accuracy)

1. Describe the uses of the data.
   There is no change in the uses of the data. OFS will use the data to respond to FOIA and PA requests. PAL will improve the ability for requesters to track and monitor FOIA requests.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern? ☒ No ☐ Yes If yes, please explain:

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   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.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☐ No ☒ Yes If yes, please list organization(s):
   Requests are referred to FOIA liaisons in SEC Divisions and Offices to provide responsive records; requests may be forwarded for response or coordination of other federal agencies; SEC Office of Information Technology (OIT) staff and contract support staff have access to the data in order to provide system administration and support.

2. Will the data be shared with any external organizations?
   ☐ No ☒ Yes If yes, please list organizations(s):
   The SEC will only share information from within the FOIA and PA program with external organizations when required by statute, executive order, regulation, or policy and for the response of a FOIA and/or PA request. This coordination may be necessary to ensure that records requested, that are not SEC records, may be responded to by the applicable federal department or agency.

   The Department of Transportation's Enterprise Services Center (DOT/ESC) has access to the system in order to process payment of fees associated with FOIA/PA requests. No other external organizations have access to the SEC's FOIA and PA information technology or paper based systems.

   Information may be shared with law enforcement, such as threatening correspondence directed at the SEC or its employees, or if an opinion is sought from an attorney at DOJ on a particular matter of FOIA or PA law.
   How is the data transmitted or disclosed to external organization(s)? Information may be transmitted via e- mail, fax or postal service. All transmission of PII conforms to SEC information handling guidance.

3. How is the shared data secured by external recipients?
   N/A

4. Does the project/system process or access PII in any other SEC system?
   ☒ No
   ☐ Yes. If yes, list system(s).

SECTION IV - Notice to Individuals to Decline/Consent Use

1. What privacy notice was provided to the different individuals prior to collection of data? (Check all that apply)
   ☒ Privacy Act Statement ☒ System of Records Notice ☒ Privacy Impact Assessment
   ☒ Web Privacy Policy ☐ Notice was not provided to individuals prior to collection

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☒ Yes ☐ No ☐ N/A
   Please explain: Persons are not obligated in any way to submit FOIA and/or PA requests to the SEC. If individuals do choose to submit a request, certain information is necessary to comply with requesting procedures for identification purposes as well as scope of request.

3. Do individuals have the right to consent to particular uses of the data?
   ☐ Yes ☒ No ☐ N/A
   Please explain: Persons are not obligated in any way to submit a FOIA and/or PA requests to the SEC. If individuals do choose to submit a request, certain information is necessary to comply with requesting procedures for identification purposes as well as scope of request. The FOIA and PA program will work with the individual and collect only the limited amount of information necessary to respond to the request.

SECTION V - Access to Data (administrative and technological controls)

1. Has the retention schedule been established by the National Archives and Records Administration (NARA)?
   ☐ No If no, please explain:
   ☒ Yes If yes, list retention period: The records are temporary; for requests without denials, the retention period is 2 years; for requests with denials, the retention period is 6 years; requests for confidential treatment are retained for 10 years, unless renewed.

2. What are the procedures for identification and disposition of the data at the end of the retention period?
   The OFS will assess records to ensure they are no longer required and will, subsequently, be disposed of at the end of the retention period.

3. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?
   OIT provides mandatory privacy and IT security training annually to all users.

4. Has a system security plan been completed for the information system(s) supporting the project?
   ☐ Yes If yes, please provide date SA&A was completed: The Security Certification & Accreditation was completed on May 16, 2013.
   ☒ No If the project does not trigger the SA&A requirement, state that along with an explanation Determination on SA&A requirement is pending.

5. Is the system exposed to the Internet without going through VPN?
   ☐ No
   ☒ Yes If yes, Is secure authentication required? ☒No ☐Yes; and
   Is the session encrypted? ☐ No ☒Yes

6. Are there regular (ie. periodic, recurring, etc.) PII data extractions from the system?
   ☒ No
   ☐ Yes If yes, please explain:

7. Which user group(s) will have access to the system?
   User groups for the FX component include: FOIA Office staff, FOIA liaisons in SEC divisions and offices, system administrators, and contractors. As a condition of their contracted service with SEC, all contractors must: sign a non-disclosure agreement; and undergo a background investigation. Authorized users will be restricted to the minimal amount of data in a record that is required to accomplish a specific job function of the user or to comply with applicable legal requirements.

   User groups for the PAL component include two types of end users: (1) users who have previously submitted a request through FX and are seeking a status of that request and (2) users who have not previously submitted a FOIA request, but are interested in the status of someone else's request. These users will only have access to information related to the status of FOIA requests.

8. How is access to the data by a user determined? Access to the information in the FX component will be determined through specified role-based permissions. These role-based access controls are based upon the principle of least privilege. The principal of least privilege states that a user may only have the minimum privileges to perform their assigned tasks. A system user, functioning as a supervisor, may assign specific rights to other users to follow the case. Access is controlled by privileges configured within the system based on the role of the individual in the business process. Access to information in the PAL component is available to users interested in tracking a FOIA request. The first type of users is individuals who have previously submitted a request through FX and are seeking a status of that request. These individuals will log in using the same username and password created when they submitted their initial FOIA request. The second type of users is individuals who have not previously submitted a FOIA request, but are interested in the status of someone else's request. In order to view the status, these users will need to input a FOIA case number.
   Are procedures documented? ☒ Yes ☐ No

9. How are the actual assignments of roles and rules verified.
   Access privileges are defined and set by the system owner in accordance with the standard operating procedures (SOP) for the system.

10. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data? Access to system is limited; audit trails and reports are monitored.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.
There is a risk that an individual submitting a FOIA and/or PA request will submit more information than is necessary, such as a SSN, when submitting a disclosure request. If more information is provided than necessary, such as the SSN, the SEC will redact and protect this information and will not enter the extraneous information into the applicable FOIA and PA system. This information will remain in the paper file but will not be further disseminated.

There is a risk of unauthorized or inadvertent release of personal information, as well as unauthorized browsing of information by FOIA and PA staff for unofficial purposes. To mitigate this risk, the SEC has: implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems; provided initial and follow-on privacy and security awareness training for each individual with access to FOIA and PA tracking systems; implemented audit trails and report monitoring that records all users' modifications and routing of records within the FOIA and PA tracking system.

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.