U.S. Securities and Exchange Commission

electronic Filings in Administrative Proceedings (eFAP)
PRIVACY IMPACT ASSESSMENT (PIA)

September 25, 2020

Office of the Secretary

Privacy Impact Assessment

electronic Filings in Administrative Proceedings (eFAP)

Section 1: System Overview

1.1 Name of Project or System

electronic Filings in Administrative Proceedings (eFAP)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted — Office of the Secretary (OS)

☐ 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:
Last updated:
Description of update:

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

☐ Enterprise 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

eFAP performs the following business function: Electronic processing for internal (i.e., SEC) and external (i.e., public) users to easily submit legal documentation in support of Administrative Proceedings (AP). The Office of the Secretary (OS) is responsible for receiving documents filed in AP and for serving notices and orders issued by the Commission and Administrative Law Judges (ALJ) in AP. OS uses eFAP, which replaces the paper filing process for APs, to electronically receive and track AP filings and facilitate the prompt distribution of public information regarding administrative proceedings. External users are required to register with login.gov, the General Services Administration's shared service that provides secure two-factor authentication (2FA), enhanced fraud detection and monitoring, to establish an eFAP user account to submit an electronic filing.

Filers may submit non-confidential or confidential documents (under seal) in the eFAP system. If a document is tagged as under seal, only users with the appropriate privileges can access documents under seal in eFAP. OS staff has the capability to correct assignments (i.e., sealed or not under seal) at any time and review submissions to ensure they are correctly classified as under seal. OS manually reviews every document and makes redactions as necessary before the documents are publicly available on https://www.sec.gov.

eFAP users are required to exclude or redact sensitive personally identifiable information (PII) from electronic filings and submissions in accordance with prescribed SEC staff e-filing procedures. SEC staff will publish e-filing procedures by the end of March 31, 2021. Prior to submitting a filing in eFAP, filers are provided notice of their responsibility to redact or omit sensitive PII and are required to attest to redaction by clicking a

checkbox on the screen before uploading documents and by clicking a checkbox before submitting the uploaded documents. Examples of PII to be excluded from submission include Social Security numbers (SSN), Taxpayer Identification Numbers (TIN), financial account numbers, credit cards or debit card numbers, passport numbers, driver's license numbers, state-issued identification numbers, home addresses (other than city and state), telephone numbers, dates of birth (other than year), names and initials of minor children, and medical information. However, if a filer believes that any of the aforementioned PII is necessary for the filing of the proceeding, the filer should file a motion for a protective order to limit disclosure of such information in accordance with *Rule 322 Evidence: Confidential Information, Protective Orders* of the Commission's *Rules of Practice* (17 CFR 201.322).

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

System Of Records Notice (SORN) SEC-36 authorities are 15 U.S.C. 77h(e), 77u, 78v, 78o(b), 80a-40, and 80b-12; the Commission's Rules of Practice, 17 CFR 201.100-900 and the Commission's Rules of Fair Fund and Disgorgement Plans, 17 CFR 201.1100-1106.

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

☒ No. However, eFAP accepts under seal documents which may, in some instances, contain SSNs.
☐ 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
SORN-36 Administrative Proceeding Files

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 the collection is to increase transparency by making filings and other information concerning administrative proceedings more readily available to the public. The primary privacy risk identified is the collection of unsolicited PII in filings and the unintentional collection of SPII. To mitigate this risk, filers must attest that any sensitive information has been redacted from the documents before uploading documents to eFAP prior to submitting the filing. In addition, OS staff manually reviews documents uploaded to eFAP and manually redacts them, as needed, prior to becoming publicly available. Documents that contain unsolicited PII necessary for a proceeding may be uploaded under seal or under a protective order to prevent unauthorized users from viewing the documents. For example, an Administrative Law Judges (ALJ) can place documents under seal so that only ALJ and OS users and certain system administrators can view the documents.

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:		

NOTE: External users must enter a telephone number when registering for eFAP access. This number is collected but is not displayed or disseminated. APTS data feeds include participants' telephone numbers and are likewise not displayed or disseminated.

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	☐ Video Recordings	☐ Voice Signature
☐ Other:		

System Administration/Audit Data

☐ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☐ Queries Ran	☐ Contents of Files
☐ Other:		

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

Name, email addresses, and telephone numbers are collected from filers for user registration purposes and to obtain contact information for sending filing review status.

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

☒ SEC Employees
Purpose: Information related to employees who file, review, or process documents in an AP.

☒ SEC Federal Contractors
Purpose: Contractors may assist OS processing duties and ENF with filing duties.

☒ Interns
Purpose: Interns may assist OS processing duties and ENF with filing duties.

☒ Members of the Public
Purpose: Information is collected from individuals registering for access to eFAP.
☐ Employee Family Members
Purpose:
☐ Former Employees
Purpose:
☐ Job Applicants
Purpose:
☐ Vendors
Purpose:
☐ Other:
Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

PII is not used for training and research efforts. Filers must attest that sensitive information is redacted from documents before uploading documents for filing submission in eFAP.

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

☐ No.

☒ Yes.
Records related to administrative proceedings are scheduled in DAA-0266-2016-0002-0005 *Congressional and Intergovernmental Correspondence and Testimony to Congress* with retention of 30 years after the case is closed. The records copy of Commission orders is not maintained in eFAP.

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

The current release of the eFAP system does not track or inform records managers of upcoming disposition decision dates. While the current process involves manual identification and disposition, retention schedule system support is anticipated after eFAP 12c upgrade in July 2021.

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 privacy risk related to the type of information collected is unauthorized disclosure of non-public information. The system allows SEC users to place documents under seal to prevent unauthorized users from viewing the documents. For example, Administrative Law Judges (ALJ) can place documents under seal so that only ALJ and OS users and certain system administrators can view the documents.

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
During registration
☒ System of Records Notice
SEC-36 Administrative Proceeding Files
☒ Privacy Impact Assessment
Date of Last Update: This is the initial PIA.
☐ Web Privacy Policy

☐ 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 those risks mitigated?

The primary privacy risk is inadequate notice to the user of the purpose of the collection that enables them to make an informed decision to provide the information requested. This risk is mitigated by providing a Privacy Act Statement at the point of information collection in eFAP. SORN-36 Administrative Proceeding Files and this PIA provide a description of the purpose and use of PII collected.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Other than collecting data for filing purposes and OS review of filing documents as discussed in Section 2.1, data is not analyzed.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: ENF, ALJ, Office of General Counsel (OGC), and other offices or divisions that need to file, review, or adjudicate documents related to an AP.

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

The primary privacy risk from internal sharing is that PII collected may be inappropriately used for an unintended purpose. This risk is minimized by employing access controls to limit access to information to only authorized users who need access to perform their job duties.

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.

There is no risk from external sharing because information in eFAP is not shared with external entities.

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): Documents can be submitted by parties to the AP or their representatives.

6.2 What methods will be used to collect the data?

Individuals submit name, email address, and phone number when registering as an eFAP user. The system has a file upload capability to accept filing documents that may contain PII.

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

The filer must verify the accuracy of the data provided. In order for registration to be completed, an email is sent to individual registrants for verification of email address.

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

☐ No
☒ Yes.
System(s): eFAP captures Name, Address, and Email from the new Administrative Proceedings Tracking System (APTS)

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 minimal risk to data quality and integrity in eFAP because only name, address, telephone number, and email address are collected directly from individuals. Access controls are in place to limit access to data based on job duties.

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.

Persons involved in administrative proceedings are required to submit all documents and other items electronically and, therefore, do not have an opportunity to decline or opt out. Users may progress with the registration process after they are informed and provide their consent.

7.2 What procedures are in place to allow individuals to access their information?

Users have access to information they submitted during registration via Update Profile functionality within eFAP and login.gov. A user may change their authentication method and email address through their login.gov profile. User name and phone number may be updated in eFAP.

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

Individuals can amend information about themselves using the Update Profile functionality within eFAP and login.gov.

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

The primary risks are lack of access to information and inability to seek redress and correction. These risks are mitigated by providing individual access or correction of information collected as expressly permitted by the Privacy Act and provided by the Freedom of Information Act (FOIA). In addition, individuals may correct information they provided using the Update Profile functionality in eFAP and login.gov.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes

8.2 Does the site have a posted privacy notice?

☐ No
☒ Yes
☐ N/A

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

☒ No
☐ Yes, but they do not collect PII

☐ Yes, and they collect PII

8.4 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

The identified privacy risk is unauthorized disclosure or unauthorized access to PII in an AP prior to a resolution. This risk is mitigated through the use of role based access control to restrict access to information in eFAP to authorized users assigned a role based on their job responsibilities.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC users complete the Privacy and Information Security Awareness training prior to being granted access to SEC information and information systems. In addition, users are trained on SEC Rules of the Road governing their activities related to safeguarding SEC information. Privacy and Information Security Awareness is provided on a continuous basis to keep users alert to privacy and security requirements and safeguards.

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

☐ No
☒ Yes
Only the user name appears in some report results where the field is available.

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

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.

Although access to this system is limited only to authorized SEC staff and registered external users (filers), the expected residual risk related to access can include the inadvertent handling or misuse of data. To mitigate this risk, role based access control is implemented to limit access to authorized users only and the type of information needed to perform job duties or submit a filing.