U.S. Securities and Exchange Commission

EDGAR Fee System Modernization (EFSM)
PRIVACY IMPACT ASSESSMENT (PIA)

March 28, 2017

Office of Information Technology

Privacy Impact Assessment

EDGAR Fee System Modernization

Section 1: System Overview

1.1 Name of Project or System

EDGAR Fee System Modernization (EFSM)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Office of Financial Management

☐ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing a replacement

First developed: 5/26/2017

Last updated:

Description of update: Replacement of the existing Momentum Sub Ledger System

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

Public companies (Registrants) are required to pay fees when they issue public debt/securities. EDGAR Fee System Modernization (EFSM) will support the processing of filing fees for fee-bearing submissions and processing refunds due to Registrants for overpayments. Additionally, EFSM will provide the capability to support financial reporting and accounting requirements. OFM's Filing Fees Branch has initiated the EFSM project, a modern Commercial Off-the-Shelf (COTS) application, to replace its current Filing Fee Sub-Ledger system which currently exists as a subsystem under EDGAR. EFSM will replace EDGAR Momentum (Fee Momentum), Offering Verification Review SharePoint site, and an Access database used to perform reconciliation.

This system will be accessed internally by OFM staff using a browser and cannot be accessed outside the SEC network. All users will be authenticated using SEC's Active Directory system. EFSM data and functions will be

authorized based on the role and authorization that each user is assigned.

The EFSM system contains bank account/payment information from Registrants. EFSM does not contain any financial information of individuals. The PII information that may be collected in EFSM is the names of individuals serving as the points of contact (POCs) or agents of Registrants, their work address, phone numbers and/or email. Filing Fees branch staff will receive SEC's training regarding protection of PII information and the safeguards that must be followed for security purposes.

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

Sections 6(b) of the Securities Act of 1933; Sections 13(e) and 14(g) of the Securities Exchange Act of 1934; and Rule 24F-2 under the Investment Company Act of 1940.

2.3 Does the project use, collect, or maintain 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

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?

There are minimal to no privacy risks to individuals whose names, work addresses, phone numbers, and emails may be contained in EFSM. Their information is collected as POC or an agent for the Registrants that are required to pay filing fees as a public company. Collecting this limited amount of PII mitigates the privacy risk to the individuals.

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	☐ 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?

POC information is collected from Registrants for purposes of processing refund requests.

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

☐ SEC Employees
Purpose:

☐ SEC Federal Contractors
Purpose:

☐ Interns
Purpose:

☒ Members of the Public
Purpose: To contact Registrants for purposes of processing refund requests.

☐ 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 testing, training, and/or research efforts. The system collects the minimally required PII to process refund requests.

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

☐ No.

☒ Yes.
There is a seven year retention schedule.

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

All of a registrants account activity will be stored in EFSM indefinitely so that registrants can receive accurate account activity statements. If EFSM is retired, then the data will be kept in accordance with the records retention schedule.

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 PII collected from individuals serving as POC or agents for Registrants is limited to name, work address, telephone, and or email. Because the information collected on individuals is limited to the data elements above, there is no significant privacy risk to the individual. Limiting the collection of information mitigates the privacy risk.

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

☐ System of Records Notice

☒ Privacy Impact Assessment
Date of Last Update: This PIA will serve as notice to individuals whose information may be in the system.

☐ 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 information collected is for the purposes of processing payments submitted by Registrants. The PII collected only relates to a POC or agent of the Registrant and is not the subject of the information collection. Privacy risks regarding notice are mitigated by this PIA which details the limited collection, purpose, and use of the information collected on the individuals.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

When a registrant requests a refund, a POC at the company is requested to address any questions about the refund request. In addition to obtaining the POC, an address or bank routing/account number where a registrant would like their refunds sent is requested. Registrants are required to request the return of unused funds (refund) using an electronic form on EDGAR to ensure that the registrant has access and authority to the EDGAR account.

5.2 Will internal organizations have access to the data?

☐ No

☒ Yes

Organizations: Division of Corporation Finance, Investment Management, and Office of Information Technology EDGAR Operations Team

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

The risk to privacy for individuals due to internal sharing is low. The POC information is maintained for the purpose of issuing a refund to the Registrants, if applicable. The primary sharing of the information collected is related to the fee submissions of the registrants and the analysis of that information with offices and divisions that have a business need for the information. This rarely includes refund information and POC information collected. . In the past seven years, there have only been a handful of cases where another office has inquired about the POC for a refund request. All information in EFSM is shared only on a need to know basis.

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.

None.

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): EDGAR, Delphi GL system and Treasury

6.2 What methods will be used to collect the data?

EFSM will interface with EDGAR to collect data from Registrants. This includes POC and agent information, and bank information. EFSM system will also receive information from Delphi GL system and Treasury. Delphi GL system and Treasury will provide general ledger and cash receipt reporting information to EFSM (primarily for reconciliation purposes).

Once the new system is in production, the data from the previous Momentum system will be migrated to and stored in EFSM.

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

EFSM relies on the registrant to provide accurate information when submitting fee submissions. In addition, SEC staff will have the capability to enter updated information into the system when necessary.

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?

Not applicable.

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.

The only individual data collected is POC information from a registrant in case there are questions about a refund request made by the registrant. It is within the discretion of the registrant to provide a POC regarding its refund request.

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

Once a refund request is submitted, the information gets sent to EDGAR and then EFSM. Individuals are not able to access the contact/bank account information provided by the registrant.

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

No

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

Given the limited purpose for collecting information for a POC, the privacy risks to the individual are minimal.

Section 8: Security

8.1 Has the system been authorized to process information?

☐ Yes
SA&A Completion Date:
Date of Authority to Operate (ATO) Expected or Granted:
☒ No
We are in the process of going through SA & A

8.2 Identify individuals who will have access to the data in the project or system and state their respective roles.

☒ Users
Roles: EFSM Staff to carry out their assigned duties; REFADMIN role to oversee the application functionality.
☐ Contractors
Roles:
☐ Managers
Roles:
☐ Program Staff
Roles:

☐ Developers
Roles:
☐ System Administrators
Roles:
☐ Others:
Roles:

8.3 Can the system be accessed outside of a connected SEC network?

☒ No
☐ Yes

If yes, is secured authentication required?	☐	No	☐	Yes	☐	Not Applicable
Is the session encrypted?	☐	No	☐	Yes	☐	Not Applicable

8.4 How will the system be secured?

It will be built and stored within the SEC IT network. Role-based access controls are implemented. Identification and authentication is enabled through Active Directory.

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

☒ No
☐ Yes
Public URL:

8.6 Does the site have a posted privacy notice?

☐ No
☐ Yes
☒ N/A

8.7 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

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

The privacy risks are minimal considering the security protections in place regarding limited access controls, identification and authorization controls through active directory and the additional security controls identified in the SA&A process.

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 staff will have to go through SEC privacy training before they have access to the system.

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

The following is recorded in the EFSM audit logs. The report and query provide details about the new records added, changes to existing records, and records deleted. The logged data is reviewed on a regular basis and retained indefinitely unless determined otherwise.

EFSM Logged Reference Data				
Accession Number	Budget Dimension	Form Type	Penalty Type	Text Code
Accounting Event	Bureau	Form Type Category	Principal	Transaction Definition
Accounting Period	CIK	Fund	Receivable Type	Treasury Symbol
Act	CIK Category	GL Account	Relationship Edit	Workflow Groups
Agency	CIK Options	GL Account Entry	Report Definition	Write-Off Reason
Agency Location Code	CIK Type	GL Account Type	Revenue Source	
Approval Template	CIR Detail Key	General System Options	Security Category	
Approval Type	CIR Inbound Crosswalk	Interest Reason	Security Organization	
BETC	Calendar Date	Interest Type	Security Role	
Bank ABA/BIC	Country	Office	Security Type	
Batch File Layout	County	Outstanding Bills	State	
Batch File Location	Disbursing Office	Payment Category	System ID	
Batch Job	Document Type	Payment Options	System Settings	
Billing Option	File Number	Payment Type	Tender Type	

9.5 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?

EFSM security model is made up of security roles which are assigned to end users. A security role defines the permitted actions that a user can execute when assigned the security role. For example, the areas of the system the user can view the type of transactions a user can process, and the work items a user can take action on. If a user attempts to perform an action that they are not permitted to take, the violation is logged and can be viewed in the Security Violations Report.

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

No residual risks are identified. The PII collected is not sensitive in nature and the security safeguards and controls in place adequately protect the PII collected.