U.S. Securities and Exchange Commission

# Auto-Certification of EDGAR Filings (ACEF)
# PRIVACY IMPACT ASSESSMENT (PIA)

**March 5, 2025**

**Office of Support Operations**

Publication History

| Revision | Date | Changes Made |
|---|---|---|
| Initial | 9/19/2017 | Original Document |
| 1 | 8/5/2020 | Review and Update |
| 2 | 11/24/2020 | Review and Update |
| 3 | 3/5/2025 | Updated for compliance with E.O. 14168 |
| | | |
| | | |
| | | |

# Privacy Impact Assessment

Auto-Certification of EDGAR Filings (ACEF)

## Section 1: System Overview

### 1.1 Name of Project or System

Auto-Certification of EDGAR Filings (ACEF)

### 1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) — Office of Support Operations (OSO)/Office of Records Management (ORMS)

☐ 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: 9/19/2017

Last updated: 11/24/2020

Description of update: Updated for compliance with E.O. 14168

### 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

☐ 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 SEC Office of Support Operations (OSO) - Office of Records Management Services (ORMS) owns ACEF and uses it to automate the process of certifying Electronic Data Gathering, Analysis, and Retrieval (EDGAR) filings requested by the public. ACEF consists of several components: the web services front end (https://www.sec.gov/forms/request_cert_filings), the SEC e-mail system which receives the e-mail request from the front end website and delivers the filings to the requestor, the m-file server (where the application resides), the Government Printing Office (GPO) where the files are certified, and SEC Feeds which moves files between the files server, web services, and the GPO. All these components together are referred to as ACEF. Information collected on the website from the requestor is stored on the ACEF server within the SEC network.

The public requestor visits the https://www.sec.gov/forms/request_cert_filings website and enters their name, e-mail address, phone number, and the accession number of the filing they are requesting. The website logic searches the EDGAR database for the requested filing. The requestor is notified whether or not the filing is found via e-mail. If the filing is found, a filing request file is sent to the ACEF Requests shared folder for processing. The m-files server picks up the request file and sends the request to https://www.sec.gov/sws/edgar/filing/. Then the filing, which may consist of multiple documents and types of documents, is returned to the m-files server. The m-files server packages the documents into a single PDF filing and sends it to the PDF Packages shared folder. From there it is picked up by SEC FEEDS and sent to the GPO where the filing is certified. SEC FEEDS picks up the certified filing from the GPO and sends it to the

CERTIFIED shared folder. The M-files server picks up the certified filing from the CERTIFIED folder and e-mails it to the requestor.

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

5 U.S.C. §552, Public information; agency rules, opinions, orders, records, and proceedings.

**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?**

Individuals who have legitimate access to PII could exceed their authority and use the data for unofficial purposes. To mitigate this risk, all SEC employees are required to take annual privacy and information security awareness training, which addresses the issues of proper handling and appropriate uses of PII. The SEC also maintains rules of behavior for employees who use SEC systems. OSO/ORMS also limits access to the PII by employing role-based access (only allowing access to users who need the particular PII to perform their duties.

## 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 |
| ☐ Sex | ☒ 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?**

The PII is necessary to establish the individual requestor's identity in order to be responsive their request for a certified EDGAR filing.

**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: Used to automate the process of certifying EDGAR filings requested by the public.

☐ 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.**

The request forms uses the minimum amount of PII needed to process the request. Requestors are limited to supplying their name, phone number, and e-mail address. This information provided by the requestor is not used for testing, training or research.

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

☐ No.

☒ Yes.
GRS 4.2 item 010 *General Information Request Files*

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

Information in ACEF is destroyed after 90 days; however, longer retention may be authorized if required for authorized business use.

**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?**

There is a risk of inadvertent disclosure of PII to unauthorized individuals. This risk is mitigated by implementing role-based access controls to limit access to authorized users who need to access the system to fulfill their job duties.

## 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
https://www.sec.gov/forms/request_cert_filings
☐ System of Records Notice

☐ Privacy Impact Assessment
Date of Last Update:
☒ Web Privacy Policy
https://www.sec.gov/privacy.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 those risks mitigated?**

There is a risk that insufficient notice is provided to the individual describing the purpose and use of the collected information. SEC mitigates this risk by providing links to the Privacy Act Statement and SEC Privacy Policy on the Request for Electronic Certification of EDGAR Filings form.

## Section 5: Limits on Uses and Sharing of Information

**5.1 What methods are used to analyze the data?**

ACEF data is not analyzed.

**5.2 Will internal organizations have access to the data?**

☒ No
☐ Yes
Organizations:

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

There is no risk to internal sharing because data is not shared with other internal divisions and offices within the SEC.

**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 data is not shared outside of the SEC.

## 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?**

The information is collected using the Request for Electronic Certification of EDGAR Filings form (https://www.sec.gov/forms/request_cert_filings) and stored in a SQL database.

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

Data collected directly from individuals using the form referenced in Section 6.2 is checked for accuracy and completeness by using field validation, re-entering their email twice, and notifying the requestor to copy and paste the accession number directly from the search EDGAR site to ensure the correct filing is requested.

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

☒ No
☐ Yes.

**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?**

The risk related to data quality and integrity is that inaccurate information may be collected. This risk is partially mitigated by using field validation, re-entering their email twice, and requiring to copy and paste the accession number directly from the search EDGAR site to ensure the correct filing is requested.

## 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 site is voluntary and is used to request public documents. If the requestor declines to provide the requested information, the request for the filing cannot be fulfilled.

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

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549-2736.

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

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736.

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

The privacy risks are lack of access to information and inability to seek redress and correction. These risks are mitigated as individuals are given the opportunity during completing the form to correct information they are providing via the email validation. Also, the SEC does not claim any Privacy Act exemptions for certified EDGAR filings. Therefore, individuals may submit a redress request as stated above.

## Section 8: Security

**8.1 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 |

**8.2 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

## 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
ORMS staff must authenticate to the system to access canned status reports.

**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, the expected residual risk related to access, given the sensitivity of the PII in the system, can include the inadvertent handling or misuse of data. To mitigate this risk, user accounts for employees are synched with SEC's Active Directory and system privileges are granted based on defined roles.