U.S. Securities and Exchange Commission

Comprehensive Financial Investigative Solution (CFIS)
PRIVACY IMPACT ASSESSMENT (PIA)

March 6, 2025

Division of Enforcement

Publication History

Revision	Date	Changes Made
Initial	11/01/2012	Original Document
1	3/24/2020	Review and Update
2	03/20/2022	Review and Update
3	03/06/2025	Updated for compliance with E.O. 14168

Privacy Impact Assessment

Comprehensive Financial Investigative Solution (CFIS)

Section 1: System Overview

1.1 Name of Project or System

Comprehensive Financial Investigative Solution (CFIS)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Division of Enforcement (ENF)

☐ 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: 11/1/2012
Last updated: 3/6/2025
Description of update: Updated for compliance with E.O. 14168

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

CFIS is a commercial off-the-shelf (COTS) product developed by Actionable Intelligence Technologies (AIT) that converts hardcopy customer financial statements and phone records into an electronic version and extracts the data into Microsoft Access and Excel for analysis. ENF uses CFIS to automate and expedite processing and integration of brokerage and bank statements. CFIS consists of two components, an application server and a structured query language (SQL) server. ENF and the Division of Exams (EXAMS) staff provide customer financial statements to CFIS technicians via email or shared folders accessible to the technicians. CFIS provides a fully automated Index-Process-Reconcile capability used to process the financial statements and return reconciled and validated data in Microsoft Excel or comma-separated values (CSV) files to ENF and EXAMS staff.

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

15 U.S.C. 77s, 77t, 78u, 77uuu, 80a-41, and 80b-9

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?

The privacy risk related to the purpose of the collection includes personal information collected without a clear purpose or without clear legal authority. This risk is mitigated by collecting information as authorized and in accordance with the collection purpose identified in SORN SEC-17.

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: Click here to enter text.		

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: Click here to enter text.		

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: Click here to enter text.		

Distinguishing Features/Biometrics

☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature

☐ Other: Click here to enter text.

System Administration/Audit Data

☒ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☐ Queries Ran	☐ Contents of Files
☐ Other: Click here to enter text.		

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

CFIS is not used to collect personally identifiable information (PII) directly from individuals. PII maintained in CFIS is used for SEC examinations, investigations, and litigation purposes.

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: Information used in CFIS is from individuals or companies under investigation by the SEC.

☐ 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 minimized as only case-related data is processed through CFIS. The data processed is provided by the investigative team and is targeted data from investigations. PII is not used for test purposes. PII from closed cases is used for training, and/or research for purposes of replicating the various outcomes of the analyses generated in real time. Data used for training is public and non-sensitive PII data.

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

☒ No.

☐ Yes.
If yes, provide the retention period and cite to the NARA schedule.

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

Not applicable.

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

☒ N/A

☐ Members of the Public

Purpose: If the system or project monitors the members of the public, explain the purpose of the monitoring.

☐ Employees

Purpose: If the system or project monitors employees, explain the purpose of the monitoring.

☐ Contractors

Purpose: If the system or project monitors contractors, explain the purpose of the monitoring.

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

The primary risk is inadvertent or unauthorized disclosure of financial information. This risk is mitigated by limiting access to such information to CFIS technicians; which use CFIS to process the financial records received from EXAMS and ENF staff.

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
SEC-17 Enforcement Files

☒ Privacy Impact Assessment Financial Investigative Software (FIS)
Date of Last Update: 9/30/2013

☐ Web Privacy Policy

☒ Other notice:
Data is associated with cases involving subpoenas. ENF provides privacy notice as part of the subpoena process.

☒ Notice was not provided.
Data is received as part of an investigation.

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 no privacy risk regarding adequate collection notice because CFIS processes information received from electronic discovery only and not directly from the public. However, for subpoenas, notice is provided in SORN SEC-17, *Enforcement Files*, PIA, and privacy notice.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Parsers (templates) are used to remove extraneous information during processing of financial statements. The Intelligent Document Analyzer capability within CFIS processes and reconcile financial statements to zero, captures data, and provides query and reporting capabilities to show the source and destination for all transactions. CFIS transfers data in PDF to Microsoft Excel for data analysis that is performed by ENF and EXAMS staff.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: The data is shared and limited to investigative staff in ENF and EXAMS. ENF receives financial productions on a weekly basis and submits data to be processed by CFIS. EXAMS receives exam data from examiners.

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

The primary privacy risk with internal sharing is inadvertent or unauthorized disclosure of PII to individuals within ENF/EXAMS who are not authorized to use CFIS. The risk is mitigated because access controls are in place to limit access to only authorized individuals who need to use CFIS to perform their job duties. In addition, PII is not stored in CFIS.

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 to privacy from external sharing because CFIS data is not shared with external organizations.

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): Financial institutions and parties to a subpoena are sources of financial data extrapolated from bank and brokerage statements.

6.2 What methods will be used to collect the data?

Data is collected and received from eDiscovery (electronic format) or in hardcopy. Hardcopy data is scanned and converted to tagged image file format (TIFF) images.

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

CFIS verifies the accuracy of the output file through reconciliation and validation of all transactions on financial statements and does not provide an output file unless all data is reconciled.

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?

The identified risk is poor data quality. If the quality of the data in the PDF provided by a financial institution is poor, the application may read incorrect numbers for transactions. The risk is mitigated because CFIS attempts to reconcile all financial transactions, produces an error, and alerts ENF staff if reconciliation fails. ENF staff must review the output, identify the error, and manually fix the transaction. In addition, ENF personnel maintain chain of custody records for the documents to demonstrate how they were received and processed, and verify the accuracy of the documents and data through testimony and litigation.

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.

There is no opportunity for an individual to consent, decline, or opt out of data collection because CFIS does not collect information directly from individuals but receives information from eDiscovery or hardcopy.

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

Individuals undergoing investigation do not have an opportunity to access information about themselves in CFIS.

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

Individuals may not access or correct information about themselves in CFIS because information about individuals under investigation for law enforcement purposes is exempt from access and correction provisions of the Privacy Act.

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. CFIS is exempt from Privacy Act provisions for individual access to information for correction because CFIS contains investigatory materials compiled for law enforcement purposes.

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 project or system involve an online collection of personal data?

☒ No
☐ Yes

Public URL: Click here to enter text.

8.3 Does the site have a posted privacy notice?

☐ No
☐ Yes
☒ N/A CFIS is not web-based.

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 the privacy and security requirements and safeguards.

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

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.