U.S. Securities and Exchange Commission

Case Information Management System (CIMS)
PRIVACY IMPACT ASSESSMENT (PIA)

May 9, 2023

Division of Enforcement

Privacy Impact Assessment

Case Information Management System (CIMS)

Section 1: System Overview

1.1 Name of Project or System

Case Information Management System (CIMS)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Division of Enforcement

☐ 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: 1/15/2011
Last updated: 12/1/2022
Description of update: Initial evaluation of an existing system.

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

CIMS is an Access 2016 database program used by analysts from the Enforcement (ENF) Information Technology Forensics Lab (ITFL) to track case-related information, including digital evidence provided by external parties, for ENF investigations. It is also used by the lab's administration group to obtain and produce work statistics used to ensure the efficient running of the lab. CIMS consists of a graphical user interface (GUI) front end that is located on the analyst's SEC computer and a SQL Server database server located on the SEC network.

CIMS uses the Access built-in forms, queries, and reports, and Visual Basic for Applications (VBA) for GUI custom programing. The database also leverages Outlook, Word, Excel, and the VBA Web Browser control for some of its capabilities.

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 and 17 CFR § 202.5

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?

Information is collected in CIMS to serve as a repository for investigations and litigation data. The privacy risk is that users may use the information in ways that are inconsistent or beyond the scope of the purpose for which the information was collected. This risk is mitigated by personnel training procedures and maintaining chain of custody records for the documents to demonstrate how they were received and processed.

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?

Personally identifiable information (PII) is collected to support investigations and litigation and to determine whether any person has violated, is violating, or is about to violate any provision of the federal securities laws or rules for which the SEC has enforcement authority. Additionally, PII may be used for any of the routine uses as set forth in SORN SEC-17 "Enforcement Files".

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

☒ SEC Employees
Purpose: The system maintains User IDs for internal auditing purposes.

☒ SEC Federal Contractors
Purpose: The system maintains User IDs for internal auditing purposes.

☐ Interns
Purpose:

☒ Members of the Public
Purpose: Information is collected from individuals and entities outside the SEC in the course of ENF investigations.

☐ 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 ENF IT Forensic Lab (ITFL) has Standard Operating Procedures (SOP) that specifically state that all data entered into CIMS must be sanitized from any sensitive information. Data is manually reviewed by ITFL branch chief and team lead before it is produced. In addition, the form used as part of our collection process does not include any SSN field. Any testing of the CIMS application will only have data without PII information and is deleted at the end of testing. Data is not used for testing or research efforts.

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

☐ No.

☒ Yes.
N1-266-09-04, items 2 and 4.

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

Data is deleted 10 years after the investigation is closed.

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 primary risk is the potential inadvertent or unauthorized disclosure of PII. This risk is mitigated by implementing access controls to limit access to those staff with a need to know. The information contained in CIMS is protected from unauthorized access through appropriate administrative and technical safeguards, which include role based access controls and encryption. The application has user roles, and all data is segregated by case/matter. Data at rest and in transit are encrypted among SEC headquarter and regional offices.

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
Date of Last Update: 2/1/2022
☐ 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?

There is a risk that individuals included in investigative materials are not made aware of the collection of their information. This privacy risk is inherent given the nature of investigative material and, often, the individuals

whose information may be found in the documents are sometimes not the providers of the information. However, the SEC has taken steps to provide transparency through publication of this PIA and SORN SEC-17.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Users can quickly and easily organize documents through the use of tags, annotation of transcripts, reports, and complex search queries. Depending on the type of documents received for a given case, they may be retrieved through use of a personal identifier. For example, emails can be searched via "From:", "To:", "Cc:", and "Bcc:" addresses, which are indexed as fields in the CIMS application. The CIMS attempts to index all document contents and metadata as text. Text searching then can be used to search for individual names and other personal identifiers. CIMS groups together collection, ligation notes, and projects with similar characteristics. The results of the data analysis may lead to new or broadened investigations of previously unknown patterns or concerns and could lead to additional enforcement actions and/or to additional document requests. Keyword searching, Boolean searching, filtering, phrases, concept groups, email threading, and cluster diagrams are tools available within CIMS for analysts to use in the course of investigations and to develop cases against potential violators. Filtering can be based on date, organization (producing party), domain name, email address, or other document metadata.

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.

The primary privacy risk with internal sharing is inadvertent or unauthorized disclosure of sensitive PII. This risk is mitigated as CIMS data is not internally shared beyond authorized ENF personnel and role-based access.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes
Organizations: Opposing attorneys during discovery phase.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

The primary privacy risk associated with external sharing is the potential risk of disclosure to unauthorized recipients during the transmission of information to external entities as part of Discovery Phase during litigation that is handled by the attorney and OIT. The SEC minimizes this risk by ensuring that electronic transmissions are secured by encryption. The CIMS application encrypts confidential data sent over an intranet. It also implements Structured Query Language (SQL) Server, which encrypts the entire session between the client and the server and allows mutual authentication. Documents are transmitted on encrypted external media or through secure file transfer methods. ENF reviews CIMS data before it is sent out by OIT and the staff attorney, to the opposing attorney to ensure whistleblower identifying information, Suspicious Activity Reports (SAR), or other Bank Secrecy Act (BSA) information is not disclosed.

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): ENF receives information from many sources during an investigation. ENF may receive documents and electronically stored information ("ESI") from other government administrative or law enforcement agencies. In an investigation, multiple requests for information could also result in information being provided by multiple individuals or branches of a corporate entity. For example, an investigation into a corporation often leads to identification of a few key document custodians. Responsive non-privileged email (emails that have been replied to) and other documents in the possession, custody, or control of the custodian are then provided to the SEC. Depending on the circumstances, documents may be provided directly by an individual or by the individual's corporate employer. As another example, investigations into trading activity often lead to account and transaction information being provided to the SEC by banks and broker-dealers.

6.2 What methods will be used to collect the data?

Documents are received by the SEC on external media, by file transfer, and as email attachments. SEC Data Delivery Standards instruct outside parties to encrypt sensitive data when providing it to the SEC.

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

The SEC maintains chain of custody records for ESI to demonstrate how they were received and processed. The accuracy of the documents and data is verified through testimony and litigation. The information received in the original correspondence is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise.

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 primary privacy risk is that information collected may be based on erroneous, inaccurate, untimely, or incomplete data. This risk is mitigated by maintaining chain of custody records for the documents to demonstrate how they were received and processed and by verifying 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.

Given the nature of the materials, individuals may not have notice as to whether their information was collected as part of an investigation. Individuals do not have the opportunity and/or right to decline to provide data and do not have the right to consent to particular uses of the data. The law enforcement exception in the Privacy Act applies.

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

Although individuals may request access to information about themselves contained in an SEC system of records through the SEC Privacy Act/Freedom of Information Act (FOIA), ENF records are exempt from the access and correction provisions of the Privacy Act (see SORN SEC-17 "Enforcement Files").

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

Individuals seeking access to any record contained in this system of records may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736. However, access to such records will likely be restricted, as the data may be 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?

Given that individuals are not generally permitted to access or correct records about themselves which are available in the CIMS application, there is a risk that inaccurate or erroneous information about an individual could be used by SEC personnel. This risk is mitigated by SEC personnel researching materials; conducting proper due diligence prior to initiating adverse action against an individual; and verifying, through testimony and litigation, the accuracy of the documents and data. This system is exempted from the Privacy Act insofar as it 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:

8.3 Does the site have a posted privacy notice?

☐ No
☐ Yes
☒ N/A

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 and contractors receive initial and annual privacy awareness training, which outlines roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that SEC employees and contractors are aware of their security responsibilities and how to fulfill them.

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.

Unauthorized access or inadvertent disclosure of information from the CIMS system could compromise ENF investigations or litigation, resulting in less enforcement of securities laws and regulations. The residual risk is low due to limited system access and data encryption technologies.