U.S. Securities and Exchange Commission

Evidence Tracking System (ETS)
PRIVACY IMPACT ASSESSMENT (PIA)

May 9, 2023

Division of Enforcement

Privacy Impact Assessment

Evidence Tracking System

Section 1: System Overview

1.1 Name of Project or System

Evidence Tracking System (ETS) 5.4.0.1

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: 12/3/2014

Last updated: 6/11/2022

Description of update: ETS v5 is the latest major enhancement of the current system including additional ENF Records Management (RM) reporting capabilities, migration of existing ENF RM Microsoft Access data to ETS, and an analysis on future ETS data archiving needs.

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

ETS, the replacement system for Testimony Tracking System (TTS), is a web-based application used by ENF Litigation Support Services (LSS) to provide a means for electronically requesting and tracking evidentiary services. The system provides the following functionality:

- Tracks requests to process evidence in support of electronic discovery and investigations
- Controls chain of custody for evidence
- Creates workflow for processing requests
- Provides a means to search request form information based on data entered
- Tracks data points associated with request forms (e.g., status, workflow state)
- Provides reporting capability

ETS routinely receives witness names, and witness IDs related to testimony from HUB by way of a custom database view. Any updates to this subset of information within HUB are updated in ETS as well.

The actual collection and processing of the digital and physical evidence files are handled by other internal SEC systems which are not within scope of the ETS effort.

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

The legal authorities that authorize the collection of source information are Sections 19 and 20 of the Securities Act of 1933; Section 21 of the Securities Exchange Act of 1934; Section 321 of the Trust Indenture Act of 1939; Section 42 of the Investment Company Act of 1940; Section 209 of the Investment Advisers Act of 1940; and 17 CFR 202.5 – Enforcement activities. Additional referenced SORN SEC-17 authorities are 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
SEC-17 Enforcement Files, 85 FR 85440 (January 27, 2021)

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 is a potential risk that information collected may be used for an unauthorized purpose. The risk is mitigated because only information collected for purposes identified in SORN SEC-17 is contained in the system and accessed only by personnel with a legitimate business need.

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: Witness ID		

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?

The case ID, witness name, witness ID, and name of the producing party (either entity or individual providing documents to the SEC) are maintained in ETS to track and manage requests for processing of evidence related activities.

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

☒ SEC Employees
Purpose: Information from Active Directory used to track and manage requests for end-user processing of evidence related activities

☒ SEC Federal Contractors
Purpose: Information from Active Directory used to track and manage requests for end-user processing of evidence related activities

☒ Interns
Purpose: Information from Active Directory used to track and manage requests for end-user processing of evidence related activities

☒ Members of the Public
Purpose: Tracking and managing requests for end-user processing of evidence related activities.

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: Former employee first name, last name and SEC email address is maintained for historical information.

☐ 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 minimum amount of PII collected is identified in section 3.1 above. Dummy PII data is used for testing and is removed from the stage environment when testing is complete. PII is not used for training or research.

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

☒ No.
There is no retention schedule because data is not deleted from the system.
☐ Yes.

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

There are no procedures for identification and disposition because ETS is not a system of records but tracks workflow status.

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 potential risk of inadvertent disclosure of PII. The risk is mitigated by encrypting data stored in ETS and limiting access to authorized users only.

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 is not provided to individuals prior to collection, but is published in the Federal Register and available on the SEC's website, www.sec.gov.
☒ Privacy Impact Assessment
Date of Last Update:
/ ☒ Web Privacy Policy

The SEC Web Site Privacy and Security Policy is provided to individuals upon logging into ETS. 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?

The primary privacy risk identified is that individuals, who provide their name when requesting evidentiary services or submitting documents to the SEC, may not be aware that their name is being maintained to track and process information in support of investigations. This risk is mitigated by publishing SORN SEC-17 and this PIA. In addition, a web privacy statement is posted on the ETS login page to provide notice to authorized users who enter information directly into ETS.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Data stored in ETS is not analyzed.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: Office of the General Counsel (OGC), Division of Examinations (EXAMS)

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

The privacy risk associated with internal sharing is that information in ETS could be inadvertently disclosed to OGC and EXAMS personnel that do not have a need to know. This risk is mitigated by role-based access control which limits authorized user access to only information needed to perform 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 a privacy risk from external sharing because data may be inadvertently disclosed. This risk is mitigated by securing sharing information pursuant to SEC-17, Enforcement Files Routine Use Disclosures.

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 provided by individual submitters

6.2 What methods will be used to collect the data?

Data is not collected directly from an individual using ETS. Documents containing data (i.e., productions) are provided by individual submitters to the SEC via email, File Transfer Protocol (FTP), United Parcel Service (UPS), Federal Express, or other delivery carriers. ENF Litigation Support Services (LSS) contractors receive and log all incoming productions.

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

Data, contained in documents provided as described in 6.2, is not checked for accuracy or completeness.

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

☐ No
☒ Yes.
System(s): Active Directory, HUB

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 to privacy related to data quality and integrity is that data collected by SEC for its investigations may be outdated or inaccurate. This risk is minimized as the data in the system is subject to review and verification by SEC attorney staff.

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 that ETS is used to support ENF investigations, individuals cannot decline to provide information or consent to use of information.

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

Individuals may request access to and correction of their information in accordance with the SEC Privacy Act/FOIA procedures by submitting a written request to FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or submit a request electronically to foiapa@sec.gov. Information used for investigatory purposes may be exempt from amendment under the Privacy Act.

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

Individuals may request access to and correction of their information in accordance with the SEC Privacy Act/FOIA procedures by submitting a written request to FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or submit a request electronically to foiapa@sec.gov. Information used for investigatory purposes may be exempt from amendment under the Privacy Act.

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

The potential privacy risk is that inaccurate data pertaining to an individual may be stored in the system and the

individual may not be able to access or amend the data. SORN SEC-17 provides notice of exemption to access and amend certain records containing 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 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

Personnel with proper privileges can run a report in the ETS application identifying the individuals' providing documents.

- Reports may be run on users, which may include first name, last name, email address, username, and login and logout times.
- Reports may be run on individuals producing documents to the SEC; and when those documents were provided to the SEC.
- Reports may be run on individuals who have had their testimony taken at the SEC and include the date of the testimony.

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

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

A residual privacy risk is over collection of personal information; this risk is assessed as low. The SEC has mitigated this risk by limiting the amount of personal information collected to only the minimal amount of personal information required to perform the functions for which the system is intended.