U.S. Securities and Exchange Commission

Information Technology Forensic Lab (ITFL)
PRIVACY IMPACT ASSESSMENT (PIA)

August 29, 2023

Division of Enforcement

Privacy Impact Assessment

Information Technology Forensic Lab (ITFL)

Section 1: System Overview

1.1 Name of Project or System

Information Technology Forensic Lab (ITFL)

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:	5/8/2018
Last updated:	
Description of update:	Previously, forensic analysis in the ITFL Forensic Analysis Network (FAN) was conducted on computers that were not connected to any network ("air-gapped'). Recently, these computers have been attached to a segregated network segment with the larger SEC computer network.

1.4 The system or program employs the following technologies. (*Check all that apply)*

☐ 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.

ITFL FAN, is an internal, isolated lab used by the Division of Enforcement (ENF) that facilitates the storage, analysis, reconstruction, and preservation of digital evidence in support of ENF investigative efforts. The lab network is segregated from the rest of the SEC network and requires specific authentication by authorized users (limited to ITFL forensic analysts). The network's connection to external resources (including the SEC network, and all other external locations) is restricted only the essential components, facilitating the Office of Information Technology (OIT) visibility into the lab for oversight and auditing reporting capabilities. This is achieved via devices within the lab through Bigfix, Splunk and Tenable on the production network. The lab does not provide access to the internet.

The lab receives electronic devices (computers and cell phones) and creates forensic images of these devices which are stored within the ITFL network. On occasion, forensic images of devices, submitted by the targets of the investigation, may also be received, and stored. The lab also stores forensic images of electronic devices that were collected by the forensic collection vendor (Agile).

ITFL FAN extracts investigative relevant data from the forensic images and produces analysis results, that may include PII. The results are loaded into the ENF's Electronic Discovery 3 (eD3) cloud system (CasePoint) for ENF investigative staff review.

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

5 U.S.C. 552a(k)(2)
17 CFR 200.312(a)(1)

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

No

2.4 Does the system or electronic collection require a Privacy Act System of Records Notice (SORN)? If yes, list the Privacy Act SORN Identifier(s)

ITFL does not create a new system of records. PII may be maintained within the ITFL which was originally collected pursuant to SEC SORN, SEC-17, Enforcement Files available at: https://www.sec.gov.gov/privacy.

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

No

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

A privacy risk related to the collection purpose is that information may be collected and used for a purpose incompatible with the original purpose of the collection. This risk is minimized because prior to the collection of a device, ENF ITFL FAN personnel consult with SEC staff to advise on the likelihood that a device may contain data relevant to an investigation, collect only those devices with a reasonable likelihood of containing relevant data, and only extract and provide for review data or files which match specific agreed-upon characteristics.

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
☒ Taxpayer ID
☐ Employee ID
☒ File/Case ID
☐ Other:

☐ Alien Registration
☐ Driver's License Number
☐ Passport Information
☐ Credit Card Number

☒ Financial Accounts
☐ Financial Transactions
☐ Vehicle Identifiers
☐ Employer ID

General Personal Data

☒ Name
☒ Maiden Name
☒ Alias
☒ Gender
☒ Age
☐ Race/Ethnicity
☒ Civil or Criminal History
☐ Other:

☒ Date of Birth
☐ Place of Birth
☒ Home Address
☒ Telephone Number
☒ Email Address
☐ Education Records
☒ Zip Code

☒ Marriage Records
☒ Financial Information
☒ Medical Information
☐ Military Service
☐ Mother's Maiden Name
☐ Health Plan Numbers

Work-Related Data

☒ Occupation
☒ Job Title
☐ Work Address
☐ PIV Card Information
☐ Other:

☒ Telephone Number
☒ Email Address
☐ Certificate/License Number
☒ Fax Number

☐ Salary
☒ Work History
☐ Business Associates

Distinguishing Features/Biometrics

☐ Fingerprints

☐ Photographs

☐ Genetic Information

☐ Voice Recording
☐ Other:
☐ Video Recordings
☐ Voice Signature

System Administration/Audit Data

☒ User ID
☐ IP Address
☐ Other:
☐ Date/Time of Access
☐ Queries Ran
☐ ID Files Accessed
☐ Contents of Files

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

PII may be collected, used, shared, or maintained to conduct SEC investigations. However, only data which meets the established search criteria provided by the ENF investigative staff is extracted as part of the ITFL FAN.

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: Data is collected to conduct SEC 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.

Information collected, including PII, 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.
DAA-GRS-2022-0009-0002

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

DAA-GRS-2022-0009-0002 identifies: Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule.

3.7 The system will monitor the following: (*Check all that apply)*

☒ 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?

Privacy risks for data collection from devices are inadvertent disclosure and unauthorized access. The risks are mitigated because only data which meets the established search criteria is provided to Enforcement's Central Processing Unit (CPU) for upload to Casepoint, which is accessed only by authorized SEC ENF staff. In addition, the ITFL FAN is segmented from the larger SEC network and access to the FAN is limited to authorized ITFL FAN users.

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.*

☒ N/A
☐ Privacy Act Statement
☐ System of Records Notice
☐ Privacy Impact Assessment
☐ Web Privacy Policy

4.2 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.

ITFL does not operate as a Privacy Act system of records. However, ITFL may process, store, maintain, disseminate, or disclose information about individuals that is collected in support of the Division of Enforcement investigative efforts pursuant to SEC SORN, SEC-17, Enforcement Files, which is available at: https://www.sec.gov.gov/privacy.

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 are not aware that their data is maintained and used as part of the ITFL. ITFL does not operate as a Privacy Act system of records. Therefore, notice in the form of a Privacy Act Statement or SORN, is not required. However, in instances where PII is obtained as part of an SEC investigation, notice is provided pursuant to SEC SORN SEC-17 Enforcement Files, which is available at: https://www.sec.gov/privacy. In addition, notice about the collection and use of information may be provided, as appropriate, source collection. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Relevant raw data is analyzed using digital forensic tools based on the investigative guidance and interrogatories provided by SEC Staff.

5.2 Will internal organizations have access to the data?

☒ No Only authorized ENF staff is provided access to ITFL full/raw forensic images and data.

☐ Yes
Organizations:

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

The risk to internal sharing is minimized because exported information is shared only with ENF investigative staff through the CasePoint, which controls SEC access and internal sharing of ITFL information.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes
Organizations: Pursuant to Routine Uses in SEC SORN SEC-17, Enforcement Files, ITFL FAN data may be shared with the Federal Bureau of Investigations (FBI); other investigative agencies working collaboratively with the SEC; and opposing counsel.

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

A privacy risk from external sharing is disclosure to unauthorized recipients during the transmission of information to external parties. This risk is minimized because external data sharing is limited to routine use disclosures outlined in SEC SORN, SEC-17, Enforcement Files. In addition, external data transmission is encrypted.

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): Devices

6.2 What methods will be used to collect the data?

Data is collected from devices using forensic hardware and software tools (such as hardware write-block devices and software tools made by market leading providers such as Cellebrite and Xways-Forensics) and methods generally accepted by the digital forensic community.

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

Data is authenticated with the original raw device or source and verified to be an accurate true copy using forensic community best practices which include the use of MD5 and SHA1 hash algorithms.

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?

There is a risk that incomplete or inaccurate information may be collected. The risk is minimized because data is forensically imaged, authenticated and verified, as described in section 6.3, prior to analysis within the ITFL FAN network.

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.

Individuals do not have the option to consent to uses, decline to provide information, or opt out of information collected for investigative purposes by ENF ITFL FAN personnel.

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

Individuals wishing to obtain information on the procedures for accessing information about themselves in the system may contact the Freedom of Information Act (FOIA)/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or may submit a request online.

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

Individuals wishing to obtain information on the procedures for correct information about themselves in the system may contact the Freedom of Information Act (FOIA)/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or may submit a request online.

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

There is a risk that individuals may have limited access or ability to correct their information. This risk is partially mitigated. Individuals can request access to information about them under the FOIA and Privacy Act. Under the Privacy Act, individuals may also request that their information be corrected. All or some of the requested information may be exempt from correction pursuant to the Privacy Act to prevent harm to law enforcement investigations or interests. However, such requests will be considered on a case-by-case basis consistent with law enforcement necessity.

Section 8: Security

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

☒ No

☐ Yes

Public URL:

8.2 Does the site have a posted privacy notice?

☒ No

8.3 Does the project or system use web measurement and/or customization technologies?

☒ No

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

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☒ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☒ 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 ITFL FAN is limited only to authorized ITFL staff, the expected residual risk related to access to PII in the system can include the inadvertent handling or misuse of data. To mitigate this risk, user accounts for employees are synced with Active Directory and system privileges are granted based on defined roles.