U.S. Securities and Exchange Commission

PenLink PLX
PRIVACY IMPACT ASSESSMENT (PIA)

March 6, 2025

Division of Enforcement

Publication History

Revision	Date	Changes Made
Initial	1/1/2015	Original Document
1	5/13/2022	Review and Update
2	3/6/2025	Updated for compliance with E.O. 14168

Privacy Impact Assessment

PenLink PLX

Section 1: System Overview

1.1 Name of Project or System

PenLink PLX

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:
Last updated: 5/13/2022
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

PenLink PLX (hereafter just referred to as PenLink) is a commercial off-the-shelf (COTS) investigative application tool used by the Center for Risk and Quantitative Analytics (CRQA), supporting the Division of Enforcement (ENF). It is used for the collection, storage, and analysis of telephonic and IP-based communications to identify risks and threats that could harm investors, markets, or regulated entities. The application converts phone records that ENF receives from telecommunication companies via subpoenas and manual processes into readable text fields, such as Excel comma-separated values (csv) files. The application is integrated with Thomas Reuter's CLEAR for obtaining telephonic information for a given phone number. ENF users may generate custom reports (i.e. call reports), tables, charts, and graphs of the analysis for use in investigations.

Key Features and capabilities of the PenLink include:

- **Pen-Proxy Add-on Module:** This module provides an encrypted connection to the external Thomas Reuters CLEAR subscription service allowing users to retrieve available information on phone numbers (e.g. owner name, address, existing carrier, and a history of carriers associated with that phone number (porting history). Once the data is retrieved from CLEAR, it is automatically populated into the PenLink case database.
- **Cell Phone Forensics:** This feature will allow for the recovery of digital evidence and data from mobile devices (e.g., seizure, acquisition, and examination/analysis processes). Staff will be able to

upload extraction reports produced by forensic imaging tools such as Cellebrite. The SEC is not currently utilizing this capability.

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.
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?

The primary privacy risk associated with the purpose of the collection is personal information may be collected without a clear purpose or legal authority. This risk is mitigated as the Federal Securities laws noted in Section 2.2 permit the collection of the information stored in PLX for enforcement-related investigations to identify risks and threats that could harm investors, markets, or regulated entities. Another risk is that ENF may collect more information than is necessary to meet the needs of a given investigation. This risk is mitigated as ENF personnel are trained to collect only mobile phone record information via subpoena or voluntary directly from the individual.

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
☒ Other: Voice Recording	☐ Video Recordings	☐ Voice Signature

Information from telephonic and IP-based systems, such as location data (GPS longitude and latitude of the approximate location from where the call was placed, and IP address of the phone, if Wi-Fi connected).

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?

PenLink stores case-related telecommunications information, i.e., mobile phone records, related to ENF investigations obtained via subpoena or other means, such as members of the public providing records to assist in the investigation.

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: Investigation and Trials

☐ 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.

Only the PII identified in section 3.1 is collected. 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.
These are non-records and therefore do not fall under NARA
☐ Yes.

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:
☐ 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 privacy risk is inadvertent disclosure of the data collected to assist with ENF investigations. This risk is mitigated by implementing role based access control, which limits authorized ENF user access to only the information needed to perform 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

☒ System of Records Notice
SEC-17 "Enforcement Files"
☐ Privacy Impact Assessment
Date of Last Update:
☐ Web Privacy Policy

☒ Other notice: SEC Form 1661 and SEC Form 1662

☐ 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 may not be aware their information may be contained within PenLink or understand how SEC uses the information collected about them. This risk is mitigated as notice of the existence, contents, and uses of PenLink is provided by the publication of the Enforcement SORN, SEC-17 and this PIA. SEC Forms 1661 and 1662 provide supplemental information regarding primary and routine uses of information provided for storage in PenLink.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

ENF personnel manually analyze information collected in PenLink for investigative purpose. Telephonic and IP-based communications are analyzed to identify risks and threats that could harm investors, markets, or regulated entities. Records that are loaded from CLEAR are manually exported into an Excel spreadsheet that is imported into various tools, such as Palantir or Casepoint for further analysis by the investigator. From these automated tools and/or manual analysis of the data, ENF users may generate custom reports with tables, charts, and graphs to support investigations.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: ENF

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

There is minimal risk to privacy from internal sharing as the information is not shared with other SEC divisions and offices. Only authorized ENF personnel are able to access information from PenLink needed to accomplish their job tasks.

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.

The sharing of PII outside of the SEC is compatible with the original purpose for collection, namely to identify risks and threats that could harm investors, markets, or regulated entities. All external sharing falls within the scope of applicable law, including the published routine uses in the SEC-17, Enforcement Files SORN.

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): PenLink converts phone records that ENF receives from telecommunication companies via subpoenas.

6.2 What methods will be used to collect the data?

Data is collected from individuals by voluntarily providing a copy of their telephone bill to ENF staff to be manually uploaded into PenLink. Information can also be received in response to a subpoena action. ENF staff manually upload information obtained from subpoenaed records. Information may also be received from a telecommunications service provider (TSP) such as CLEAR. When ENF staff submit an inquiry to CLEAR, the information listed in 3.1 about a phone number is returned and automatically populated in the PenLink database.

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

Other than system data validation for field data type (e.g. character or numeric), there are no system checks for accuracy or completeness of data received from CLEAR or information manually entered by ENF staff into the PenLink database. ENF staff using other documents collected in the case and data discovered during the course of the investigation verify information manually entered.

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 privacy risk that PenLink may contain inaccurate or outdated information. This risk is minimized because information collected voluntarily from the individuals or via subpoena is assumed to be accurate. It is also assumed that information received from CLEAR and other systems was checked for quality and integrity at the original point of collection.

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.

Where information is sought voluntarily, individuals may decline to provide information for use in PenLink. Individuals do not have the opportunity to consent, decline, or opt out of providing information where it is sought by subpoena, discovery, or other legal provision.

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

Information collected and stored in PenLink for investigation or litigation purposes is exempted from the Privacy Act provision for access to records. Otherwise, individuals seeking to obtain information on the procedures for gaining access to the contents of records may contact the 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 or online.

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

Information collected and stored in PenLink for investigation or litigation purposes cannot be amended directly by an individual. Individuals wishing to obtain the procedures for amending information about themselves in PenLink that is voluntary and not tracked for investigation or litigation purposes may contact the 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 or online.

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

There are no identified privacy risks related to individual participation. No mitigation actions are recommended. SORN SEC-17 provides notice of exemption to access and amendment of 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

Users can generate reports, tables, charts, and graphs in PenLink using templates, or make customized reports based on their own desired criteria (i.e. names, phone numbers, and incoming/outgoing call records) for an investigation analysis.

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 PenLink is limited only to authorized SEC ENF 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 all SEC employees and contractors are synched with Active Directory and system privileges are granted based on defined roles.