U.S. Securities and Exchange Commission

Legal Files – Office of Inspector General (OIG)
PRIVACY IMPACT ASSESSMENT (PIA)

February 22, 2022

Office of Inspector General

Privacy Impact Assessment

Legal Files-OIG

Section 1: System Overview

1.1 Name of Project or System

Legal Files - Office of Inspector General (LF-OIG)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) OIG

☐ 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: 6/27/2017

Last updated: 1/10/2020

Description of update: Legal Files-OIG was upgraded to version 10.6 to support the use of TLS 1.2.

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

LF-OIG is used by the SEC Office of Inspector General to support functions related to providing legal guidance and representation for the Commission. The system provides the following:

- Case Management: Helps OIG track and provide reporting on its cases. Users have the ability to open, modify, assign, and close a case.
- Document Management: Provides the capability for users to add, update, and delete documents associated with a case.
- File Search: Allows users to easily find and retrieve files, cases, and other relevant information contained in the system using all available field identifiers (such as case type, employee assigned, date, case number, and case name), metadata, and other attributes. In addition, users may perform a full text search on case, folder, and file content.
- Records Management and Retention: Files and cases are federal records subject to a particular records retention schedule, which includes procedures for disposing of federal records contained in the system.
- Reporting: Enable users to create and save custom/ad hoc reports.

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

Inspector General Act of 1978, as amended, through P.L. 114-317, 5 U.S.C. app., and specifically 5 U.S.C. app. Section 8G(g)(4)

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:	Social security numbers of persons related to investigations may be contained in files relevant to legal matters on which OIG provides support and in Appellate and Adjudication case files. In addition, Social Security numbers may be contained in personnel files relevant to employment cases handled by OIG.
If yes, provide the legal authority:	Inspector General Act of 1978, as amended, through P.L. 114-317, 5 U.S.C. app.

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-18 Office of Inspector General Working Files

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 risks related to the purpose of the collection include personal information is 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-18.

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?

PII is collected, used, shared and maintained to support and manage investigations related to SEC programs, operations, and OIG matters.

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

☒ SEC Employees
Purpose: May be factually relevant in employee misconduct investigations and related matters handled by OIG.

☒ SEC Federal Contractors
Purpose: May be factually relevant in investigations or audit matters handled by OIG.

☒ Interns
Purpose: May be factually relevant in investigations or audit matters handled by OIG.

☐ Members of the Public
Purpose:

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: May be factually relevant in investigations or audit matters handled by OIG.

☒ Job Applicants
Purpose: May be factually relevant in investigations or audit matters handled by OIG.

☒ Vendors
Purpose: May be factually relevant in investigations or audit matters handled by OIG.

☐ 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.

OIG staff ensure that the minimum amount of PII is collected for use and storage in the system. PII is not used for testing, training, and /or research efforts.

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

☐ No.

☒ Yes.

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

LF-OIG records are maintained until they become inactive, at which time they are retired or destroyed in accordance with record schedule DAA-0266-2018-0002. Records that have reached the end of their retention period are identified by the Business Owner or designated OIG personnel.

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 or unauthorized access/disclosure of PII and other non-public information. This risk is mitigated by implementing access control and limiting the number of users to less than fifteen (15) OIG 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.*

☐ Privacy Act Statement

☒ System of Records Notice
SEC-18

☐ Privacy Impact Assessment
Date of Last Update:

☐ 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?

The primary privacy risk is individuals may not have notice on the use of their information stored in LF-OIG. This risk is mitigated by ensuring that applicable SORN SEC-18 is current and adequately covers the categories of records and individuals.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Data is manually analyzed via search and reporting capabilities, which may present existing information in the form of graphs, charts, and related management metrics. The application does not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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.

There is no privacy risk from internal sharing because information is not shared with organizations outside of OIG.

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 privacy risk from external sharing because information 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): Information may be obtained from SEC Divisions and Offices.

6.2 What methods will be used to collect the data?

Depending on the type of OIG matter, information may be collected by subpoena or discovery, OIG staff collecting information directly from the individual, or provided by other Offices or Divisions. Data is entered into the system by OIG staff.

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

The data in the system is subject to supervisor and peer review checks for accuracy on a case-by-case basis. Information collected from individuals that is subject to an adversarial process also provides the individuals opportunities to address accuracy and completeness during that process.

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 of obtaining outdated or inaccurate information resulting from the data sources and methods of collection. This risk is minimized because data is collected directly from the individual by OIG staff. In addition, information collected by subpoena or discovery may be corrected by the individual during the litigation process or by OIG staff during supervisory/peer review of case information.

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 to be included in Legal Files is sought voluntarily, individuals may decline to provide information. 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 LF-OIG for investigation or litigation purposes is exempted from the Privacy Act provision for access to records, as noted in SORN SEC-18. Otherwise, individuals wishing 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 may submit online.

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

Information collected and stored in LF-OIG for investigation or litigation purposes cannot be amended directly by an individual. Individuals wishing to obtain the procedures for amending information about themselves in LF-OIG 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-18 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-related 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

9.6 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 OIG 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.