U.S. Securities and Exchange Commission

Investigations Management Information System (IMIS)
PRIVACY IMPACT ASSESSMENT (PIA)

November 9, 2014

Privacy Impact Assessment
Investigations Management Information System (IMIS)

General Information

1. Name of Project or System.
   Investigations Management Information System (IMIS)

2. Describe the project and its purpose or function in the SEC's IT environment.
   IMIS is a case management system that will allow OIG staff to administer and track case and complaint information in a uniform manner from a single repository. IMIS assists the OIG in receiving and processing allegations of violation of criminal, civil, and administrative laws and regulations relating to SEC employees, contractors, grantees, and other individuals and entities associated with SEC. The IMIS system will be used to centralize collaboration and location of case documents and enhance management oversight refining the OIG's case matrix business processes.

3. Requested Operational Date? The IMIS system has been operational since 2/24/2014. This PIA assesses the privacy risks and vulnerabilities of the data collected.

4. System of Records Notice (SORN) number? SEC-43, Office of Inspector General Investigative Files

5. Is this an Exhibit 300 project or system? ☒ No ☐ Yes

6. What specific legal authorities, arrangements, and/or agreements allow the collection of this information? Inspector General Act of 1978, as amended, Pub. L. 95-452, 5 U.S.C. App.

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   IMIS has searchable data fields, including name, address, social security number (SSN), telephone number, date of birth, email address, zip code. Information about individuals may also be discovered in "free-text" fields and other scanned paper investigative files, which vary depending on the particular investigation.

2. Does the project/system use or collect the social security number (SSN)? (This includes truncated SSNs)
   ☐ No.
   ☒ Yes. If yes, provide the function of the SSN and the legal authority to collect.
   Inspector General Act of 1978, as amended. Where the identification number is the social security number, collection of this information is authorized by Executive Order 9397.

3. What are the sources of the data?
   Information is collected from individuals regarding complaints of criminal, civil, or administrative violations, including, but not limited to individuals alleged to have been involved in such violations; individuals identified as having been adversely affected by matters investigated by the OIG; and individuals who have been identified as possibly relevant to, or who are contacted as part of an OIG investigation.

Information is also collected from sources other than the individual, because investigations require verification and confirmation of information through third parties.

4. Why is the data being collected?
   SEC OIG collects information in order to meet its responsibilities under the IG Act to conduct investigations relating to SEC programs and operations. OIG collects information only where OIG has specific legal authority to do so and the information is required to meet OIG's responsibilities, including those expressly established under the Inspector General Act. OIG collects SSNs to verify the identity of subjects, complainants, witnesses, and third parties.

5. What technologies will be used to collect the data?
   IMIS is a Web based system allowing multiple database users; the ability to search the database; and enhanced reporting capabilities. OIG investigators collect and analyze information through a number of techniques, including interviews of complainants, witnesses, victims, and subjects; reviews of records (e.g., personnel files, contract or grant files, and financial records); collection of forensic evidence; surveillance and consensual monitoring; and use of computer technology (e.g., link analysis, databases, spreadsheets, cyber forensics, and data mining)

SECTION II - Attributes of the Data (use and accuracy)

1. Describe the uses of the data.
   OIG uses information maintained in this system of records in order to conduct investigations relating to SEC programs and operations. OIG's most common use of such information, including social security numbers (SSN), and other PII is to confirm the identity of individuals. OIG uses SSN to confirm identities; to trace people, assets, and transactions; and other permissible purposes. The specific use depends on the allegation under investigation. OIG collects information only where OIG has specific legal authority to do so and the information is required to meet OIG' responsibilities, including those expressly established under the Inspector General Act. OIG collects SSNs to verify the identity of subjects, complainants, witnesses, and third parties; to use as a search term in searching public and non-public databases for information relating to the case; and for other investigative purposes.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern? ☐ No ☒ Yes If yes, please explain: OIG's collection is restricted to areas of the case and is analyzed to confirm case facts and the revealing of concerns and patterns of the case. In some instances, the data mining occurs primarily for statistical and case management purposes. For example, OIG may review data to track trends in terms of pending and completed investigations, types of complaints received, and various other factors in order to analyze office and personnel needs for the OIG.

   OIG also compiles information relating to investigative statistics for various reporting requirements, including but not limited to, the Semi-Annual Report to Congress required under the Inspector General Act, 5 U.S.C. App. 3, § 5.

OIG also reviews data to evaluate incoming complaints and to respond to various Congressional, law enforcement and litigation requests, and information requests by other Federal agencies and U.S. Attorneys' offices during the course of a criminal prosecution or civil enforcement action.

The IMIS can be used to cross-check various terms, such as name, case number, subject of investigation, alleged statutory or regulation violation, employing SEC Organization, results, status, special agent assigned, and date of complaint and of closing, in order to verify information, generate reports, and ascertain relationships between complaints, complainants, assignments, and other investigative matters.

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   SEC OIG has an intense editing and review process for all OIG Reports of Investigations. Agents are instructed to ensure accuracy and thoroughness through the investigative process; to consider confidentiality and security issues; to include disclosure caveats where appropriate; and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation. Data extraction and collection is primarily from government systems and were possible crossed checked through more than one system. In addition, the use of law enforcement and public databases are used to verify accuracy of information. Methods may also include reference to commercial databases to: obtain background information; verify addresses, identities, and contact information; trace proceeds from illegal activities; identify possible witnesses; and for other investigative purposes. In addition, each record has a unique file number to prevent duplication. OIG verifies records by checking every incoming complaint to ensure that OIG has not received the same complaint previously. If so, OIG cross-references the two complaints; if not, the complaint is processed as a new entry. Information contained in the complaint is verified through the investigative process, which varies depending on the allegation and information at issue. OIG also updates the IMIS with timely information on referrals, administrative actions, prosecutions, civil enforcements, and other information addressing the status of, or results of, an investigation or complaint review.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☐ No ☒ Yes If yes, please list organization(s): OIG shares information in IMIS and related paper files with other SEC organizations, as needed. Such information is shared on an as needed basis, depending on the particular persons and programs under investigation, and on whether a particular complaint, case, or allegation is referred for further action or for information, and to obtain information pertaining to the OIG investigation.

2. Will the data be shared with any external organizations?
   ☐ No ☒ Yes If yes, please list organizations(s): The specific external organizations with which SEC OIG shares IMIS information and OIG investigative paper files externally, depend on the nature, subject, status, and other factors unique to each investigation. Such

agencies include other Federal law enforcement agencies; State and local police departments. If a case is referred for prosecution, information will be shared with the Federal, State, or local prosecutors. Information may also be shared with Congressional Committees with jurisdiction over matters under investigation.

How is the data transmitted or disclosed to external organization(s)? OIG transmits information in a variety of ways, including electronically, in oral briefings and interviews, in writing, by telephone, hand delivery and certified mail service. The method of transmission depends on the nature of the information, including its privacy interests, status of the investigation, and confidentiality. Personnel who maintain the IMIS do not have direct access to OIG investigative paper files.

3. How is the shared data secured by external recipients?
   Information is shared primarily with other law enforcement agencies and government agencies with personnel who are already familiar with the Privacy Act and other restrictions on release of information. OIG notifies recipients of the confidential nature and disclosure restrictions through verbal statements, written markings on documents, and agency policies recognizing the confidential nature of such materials. SEC OIG closely follows and is attuned to Privacy Act requirements and other confidentiality concerns in sharing information with other Federal and State agencies. Access is strictly limited to authorized persons with a need to know, who require access to perform their official duties.

4. Does the project/system process or access PII in any other SEC system?
   ☒ No
   ☐ Yes. If yes, list system(s).

SECTION IV - Notice to Individuals to Decline/Consent Use

1. What privacy notice is provided to the different individuals prior to collection of data? (Check all that apply)
   ☒ Privacy Act Statement ☒ System of Records Notice ☒ Privacy Impact Assessment
   ☐ Web Privacy Policy ☒ Notice is not provided to individuals prior to collection
   Please Explain: The publication of this PIA and the System of Records Notice SORN SEC-43, Inspector General Files (see 79 FR 30661, July 7, 2014) provide public notice of the collection, use, and maintenance of this information. Affirmative Privacy Act (e)(3) notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants. The final rule for the system of records officially exempts the system from portions if the Privacy Act adopted in 40 FR 44068 (September 24, 1975).

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☒ Yes ☐ No ☐ N/A

Please explain: Individuals have the opportunity and/or right to decline to provide information depending on the nature of the investigation. OIG investigators undergo extensive training on interviewees' rights and obligations in the context of responding to OIG investigative inquiries, and OIG has policies and procedures in place addressing interviewees' rights and obligations that vary depending on the type of investigation and on whether the interviewee is a Federal employee.

3. Do individuals have the right to consent to particular uses of the data?
   ☒ Yes ☐ No ☐ N/A
   Please explain: Depending on the nature of the investigation, OIG investigators may ask persons if they wish to consent to particular use of the information they provide – for example, whomever requests confidentiality will be advised of the extent to which confidentiality can be provided under applicable laws and regulations.

SECTION V - Access to Data (administrative and technological controls)

1. Has the retention schedule been established by the National Archives and Records Administration (NARA)?
   ☐ No If no, please explain:
   ☒ Yes If yes, list retention period: Records in this system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration.

2. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?
   All SEC staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII. Only OIG staff will access and use the IMIS application. Staff in the Investigative Branch of the OIG receives additional training on IMIS application.

3. Has a system security plan been completed for the information system(s) supporting the project?
   ☒ Yes If yes, please provide date SA&A was completed: 2/19/14
   ☐ No If the project does not trigger the SA&A requirement, state that along with an explanation

4. Is the system exposed to the Internet without going through VPN?
   ☒ No
   ☐ Yes If yes, Is secure authentication required? ☐ No ☐ Yes; and
   Is the session encrypted? ☐ No ☐ Yes

5. Are there regular (i.e., periodic, recurring, etc,) PII data extractions from the system?
   ☐ No
   ☒ Yes If yes, please explain: IMIS can be used to cross-check various terms, such as name, case number, subject of investigation, alleged statutory or regulation violation, employing SEC Organization, results, status, special agent assigned, and date of complaint and of

closing, in order to verify information, generate reports, and ascertain relationships between complaints, complainants, assignments, and other investigative matters.

6. Which user group(s) will have access to the system?
   User groups with access to the system are SEC OIG Staff assigned to the Investigative Branch. Each employee with access must first have a valid OIG network account and then an individually identifiable IMIS account.
   Access to OIG investigative paper files are restricted to OIG Investigative Branch personnel assigned to the case, the OIG branch that is handling the investigations, OIG management, and other OIG personnel as required. The system will have a single user sign on but each valid user will be assigned specific roles. Roles are defining operational permissions of three classes of users from the least role to system administrator. The roles are Investigator, Supervisory and Administrator. Access is limited to OIG staff only.

   Additionally, OIG IT Division has contractors providing programming support for IMIS, and OIT's contractors provide general IT and programming support to OIG as an organization. Contractors do not have access to paper investigative files.

7. How is access to the data by a user determined?
   Through roles and permissions, each OIG employee who is given an IMIS account is assigned privileges in order to restrict access to specific case files, including the ability to write and read each case record.

   Are procedures documented? ☒ Yes ☐ No
   OIG has established procedures for requesting access to IMIS. Each OIG employee assigned to the Investigative Branch is given an OIG network account after the employee's clearance has been validated.

8. How are the actual assignments of roles and rules verified?
   System administrative officer submits all access requests and levels of access through the OIG chain-of-command for approval and verification.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
   IMIS will not allow unauthorized browsing based on the staff's permissions and roles. In addition, a system of periodical review of all staff roles and permissions subjected to senior staff confirmation of access occurs and is recorded.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

Privacy risks involve the potential for misuse of data or unauthorized access to data. To mitigate this risk:

- IMIS information and OIG investigative paper files are closely safeguarded in accordance with applicable laws, rules and SEC policies, including SECR 24-08, Management and Protection of Privacy Act Records and other PII.
- The IMIS file server and Investigations paper records are located in a controlled secure zone to provide a layer of physical security to the server, backup tapes, and paper records. Access is strictly limited to authorized staff that requires access to perform their official duties. File areas are locked at all times or kept in otherwise secure areas, and facilities are protected from the outside by security personnel.
- Records are also protected from unauthorized access through appropriate technical safeguards, including multi-layer firewall architectures, access codes, and passwords. Each user has an account established within IMIS and gains access to the system using a logon name and password on a secure network. Each authorized user is provided with a limited permission level based upon their position and need to know.
- Data is secure in accordance with FISMA requirements and has had the required Security Assessment and Authorization, signed on 2/19/14.

Privacy risks associated with inaccurate or untimely information may result as information is not always collected directly from the individual involved; information could be used in a manner inconsistent with established OIG privacy policies; and the individual may not be aware that information relating to him/her is being compiled by OIG. To mitigate these privacy risks

- OIG conducts its investigations with due professional care, as follows:
- Investigations are conducted in a diligent and complete manner, taking reasonable steps to ensure sufficient relevant evidence is collected; pertinent issues resolved; and appropriate administrative, civil, and criminal remedies are considered.
- Investigations are conducted in accordance with applicable laws and regulations, prosecutorial guidelines; OIG policy and procedures; and with due respect for rights and privacy of those involved.
- Evidence is gathered and reported in an unbiased manner.
- Investigations are conducted in a timely manner based on the variables and complexities involved in each case, and are supported with appropriate documentation.
- Appropriate investigative techniques are employed to ensure data gathered is sufficiently reliable for making judgments regarding the matters being investigated.
- Sources of investigative information are documented in sufficient detail to provide a basis for assessing its reliability.
- Data gathered and analyzed as part of the investigation is accurately interpreted, logically presented, and maintained in the investigative case file.
- In addition, OIG has published a revised SORN SEC-43 (see 79 FR 30661, July 7, 2014) which, along with this PIA, provides additional information to inform individuals about the contents and purposes of IMIS.

Privacy risks associated with external sharing may vary depending on the nature of the investigation and parties/entities involved. Risks are mitigated by:

- Proper markings on documents;
- Requirements for secure access; and

- Appropriate transmittal mechanisms that vary depending on the nature of the information, and the vehicle by which it is transmitted.