U.S. Securities and Exchange Commission

Office of Inspector General – Case Management System (OIG-CMS)
PRIVACY IMPACT ASSESSMENT (PIA)

May 12, 2023

Office of Inspector General

Privacy Impact Assessment

Office of Inspector General – Case Management System (OIG-CMS)

Section 1: System Overview

1.1 Name of Project or System

Office of Inspector General – Case Management System (OIG-CMS)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) — Office of Inspector General

☐ 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:	11/17/2019
Last updated:	11/17/2019
Description of update:	Updated to SQL Server 2019.

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

The Office of the Inspector General (OIG) is an independent office within the Securities and Exchange Commission (SEC) that conducts, supervises, and coordinates audits, evaluations, investigations, and other reviews of the Commission's programs and operations. OIG-Case Management System (CMS) is internally hosted and leverages Wingswept Case Management and Tracking System (CMTS), a commercially off the shelf (COTS) application designed to support OIG's Office of Investigations (OI). The system provides case management, basic document repository, and records management capabilities for OI. Only OIG personnel are authorized to use OIG-CMS.

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

Inspector General Act of 1978, as amended, Pub. L. 95-452, 5 U.S. C. App.

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:	The SSN is collected as a part of the investigative identification and document collection.
If yes, provide the legal authority:	Inspector General Act of 1978, as amended, Pub. L. 95-452, 5 U.S. C. App. Where the identification number is the SSN, collection of this information is authorized by Executive Order 9397.

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 is that individuals may not be aware that their information is collected in an SEC system of records for the purpose of case management. This risk is mitigated by the publishing of the SORN SEC-18, OIG Working Files. The SORN provides public notice to individuals of the collection of information and its uses at the SEC.

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 to enable the OIG to investigate allegations of criminal, civil, and administrative violations relating to SEC programs and operations by SEC employees, contractors, and outside entities. In addition, PII may be used by the OIG to identify vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's programs and operations.

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

☒ SEC Employees
Purpose: SEC employee information is collected and used to conduct a complete criminal, civil, or administrative investigation.

☒ SEC Federal Contractors
Purpose: Same as SEC employees.

☒ Interns
Purpose: Same as SEC employees.

☒ Members of the Public
Purpose: Information from members of the public is collected and used to conduct a complete criminal, civil, or administrative investigation.

☒ Employee Family Members
Purpose: Same as SEC employees.

☒ Former Employees
Purpose: Same as SEC employees.

☒ Job Applicants
Purpose: Information from job applicants is collected and used to conduct a complete criminal, civil, or administrative investigation.

☒ Vendors
Purpose: Vendor information is collected and used to conduct a complete criminal, civil, or administrative investigation.

☐ 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.

PII is minimized in the system by only collecting information necessary to investigate allegations of criminal, civil, and administrative violations. 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.

DAA-0266-2018-0002, Depending on the investigative record type, record schedules are permanent; temporary 10 years; and temporary 3 years.

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

OIG personnel annually review, identify and retain matters by the date of closure. In addition, OIG–CMS has a notification feature that selects and identifies the record type for each matter; which helps to identify matters nearing the end of the retention period.

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 privacy risk related to the type of information collected is inadvertent disclosure or unauthorized access to sensitive PII. The risk is mitigated by role based access controls in place to limit system access to authorized users based on job role.

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
When collecting information from individuals in a voluntary capacity, OIG personnel verbally inform individuals that providing information is voluntary. In instances where individuals are required to provide information, OIG personnel provide a written Privacy Act Statement to the individuals.
☒ System of Records Notice
SEC-18 Office of Inspector General Working Files
☒ Privacy Impact Assessment
The OIG-CMS PIA is not provided to individuals prior to collection, but is published on the SEC's website, www.sec.gov.
Date of Last Update: 9/17/2019
☐ 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?

Adequate notice is provided because a Privacy Act Statement is provided in written and verbal forms to individuals and SORN SEC-18 is published in the Federal Register and accessible from the agency's website.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Data in OIG-CMS is not analyzed.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: Internal SEC divisions and offices do not have access to OIG-CMS. However, reports containing information may be shared with internal SEC divisions or offices as needed for OIG investigation.

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

Privacy risk from internal sharing of information is minimal because only investigatory reports are shared with divisions and offices as described in section 5.2.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes
Organizations: External organizations do not have access to OIG-CMS. However, information may be shared with investigative and law enforcement organizations when necessary.

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

The privacy risk from external sharing is minimal because external organization do not have access to OIG-CMS and information is only shared externally for investigative and law enforcement purposes.

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): Only authorized OIG personnel enter information about individuals into OIG-CMS.

6.2 What methods will be used to collect the data?

Methods used to collect information are interviews, data requests, emails, subpoenas, and law enforcement databases.

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

The information received from sources identified in section 6.2 is assumed to be true and accurate, unless additional information obtained from other sources is contradictory. When data is collected by interviewing individuals or entities during an investigation, the individuals or entities are responsible for ensuring the accuracy of the data provided. OIG personnel may verify information and follow up with individuals if information is found to be inaccurate.

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 discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

The privacy risk related to data quality and integrity is inaccurate information being collected from the data sources such as interviews, data requests, emails, subpoenas, and law enforcement databases. The risk is mitigated by OIG personnel collecting the data directly from the individual or entity. In addition, information collected by subpoena or discovery may be corrected by the individual during the interview process where OIG personnel can update the information provided.

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.

In general, individuals do not have the opportunity to consent to the uses of their information in OIG-CMS because the system is used for investigative and/or law enforcement purposes. However, individuals who are interviewed in a voluntary capacity may decline to provide information. Individuals who are the subject of an investigation may not decline or opt out of providing information. These individuals are provided written notice of their obligation to provide information.

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

Individuals who are under investigation by OIG or law enforcement are not allowed access to their information in OIG-CMS. Individuals who are not under investigation may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736.

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

Individuals do not have direct access to OIG-CMS to amend information about themselves. If they are under investigation, their information cannot be amended in the system. Individuals not under investigation may submit a request in writing to the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736 or may submit a request electronically to foiapa@sec.gov.

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. 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	☐ N/A
Is the session encrypted?	☐ No	☐ Yes	☐ N/A

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 The reports will contain very limited PII (such as a name) if necessary for purposes of issuing the report

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.

Safeguards, including access controls, encryption, firewalls, and other security mechanism are in place on the SEC network to protect data in OIG-CMS and minimize residual risk related to access.