U.S. Securities and Exchange Commission

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

September 17, 2019

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)

☐ 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:
Description of update:

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

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-CMS leverages Wingswept Case Management and Tracking System (CMTS), a commercially off the shelf (COTS) application designed to support OIG law enforcement operations. OIG-CMS will be internally hosted. The system will provide case management, basic document repository, and records management capabilities for the OIG's Office of Investigations (OI) staff. Only staff of OIG will be authorized to use the system. OIG-CMS will replace the current IMIS system. Data from IMIS will be imported into the new system or archived in accordance with the data's record retention schedule and IMIS will be retired.

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-43 OIG 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 and the purpose of the collection. This risk is mitigated by the publishing of the SORN SEC-43, OIG Files. The SORN provides public notice to individuals of the collection of information and its uses at the SEC. This PIA and the SORN provide the legal authority allowing the collection of information and the legal requirements for the use of that information.

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?

The PII is necessary for the OIG to investigate allegations of criminal, civil, and administrative violations relating to SEC programs and operations by SEC employees, contractors, and outside entities. The information may also aid OIG in identifying vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's program and operations

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

☒ SEC Employees
Purpose: Provide information necessary for a fair, thorough, and accurate, or complete criminal, civil, or administrative investigation.

☒ SEC Federal Contractors
Purpose: Provide information necessary for a fair, thorough, and accurate, or complete criminal, civil, or administrative investigation.

☒ Interns
Purpose: Provide information necessary for a fair, thorough, and accurate, or complete criminal, civil, or administrative investigation..

☒ Members of the Public
Purpose: Provide information necessary for a fair, thorough, and accurate, or complete criminal, civil, or administrative investigation.

☒ Employee Family Members
Purpose: Provide information necessary for a fair, thorough, and accurate, or complete criminal, civil, or administrative investigation.

☒ Former Employees
Purpose: Provide information necessary for a fair, thorough, and accurate, or complete criminal, civil, or administrative investigation.

☒ Job Applicants
Purpose: Provide information necessary for a fair, thorough, and accurate, or complete criminal, civil, or administrative investigation.

☒ Vendors
Purpose: Provide information necessary for a fair, thorough, and accurate, or 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 will not be 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.
Need to determine how to address NARA when operational requirements

☒ Yes.
N1266052. Depending on the investigative record type, record schedules are permanent; temporary 10 years; and temporary 3 yr.

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

OIG staffers annually review, identify and retain matters by the date of closure. OIG will explore deploying a notification feature within the new OIG-CMS to select and identify the record type for each matter to aid in efficiently identifying 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 is that personally identifiable information collected in the course of an investigation may be unnecessary or excessive. This risk is mitigated by limiting the collection of information to that which is necessary to thoroughly and fairly conduct investigations. Additionally, the system will assist the OIG in identifying and disposing of information in a timely manner and thus not maintaining information longer than necessary.

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 staffers inform the individuals orally that the information is voluntary. In instances where individuals are required to provide the information, OIG staffers provide written notice to the individual that providing the information is mandatory.

☒ System of Records Notice
SEC-43

☒ Privacy Impact Assessment
Date of Last Update: TBD

☐ 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 privacy risk is that individuals providing information to OIG staffers is inadequate to inform them of the uses of the information. This risk is mitigated by publishing the applicable SORN SEC-43, OIG Files, in the Federal Register and posting on the agency's website, SEC.gov. Additionally this PIA will be made publicly available on the SEC.gov website. Also, OIG staffers provide verbal or written notice, as required, to individuals when collecting information directly from them.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

OIG collects information from various sources to include interviews, data requests, emails, subpoenas, law enforcement databases, SEC databases, and public databases in the course of an investigation. The information collected is used to support matters resulting in criminal prosecutions, fines, civil penalties, administrative sanctions, and personnel actions. The information may also aid OIG in identifying vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's program and operations.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: Internal organizations do not have access to OIG-CMS. However, limited information may be shared with internal divisions or offices as needed or required in furtherance of the investigative mission and requirements of the OIG. Information shared will be contained in investigatory reports summarizing findings. The reports will contain very limited PII (such as a name) if necessary for purposes of issuing the report.

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

The privacy risk is that information may be shared with SEC personnel, who do not have a need to know the information in the course of their duties. This risk is mitigated by limiting access to OIG-CMS to OIG staffers only. Also, will only share investigatory reports with affected offices or divisions as necessary to carry out its business function. The reports will contain the minimally require PII necessary for issuing the report.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: External organizations do not have access to OIG-CMS. However, limited information may be shared with prosecuting organizations and law enforcement organizations only as needed or required in furtherance of the investigative mission and requirements of the OIG.

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

The privacy risk is unauthorized access or unauthorized disclosure. This risk is mitigated by only sharing information with prosecuting or law enforcement organizations as necessary to support OIG's mission. Information shared will be contained the minimum amount of PII necessary to coordinate the investigation with the external organization. External organizations will not have access to the system. OIG staffers will generate investigatory reports to provide relevant information.

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): Interviews, emails, subpoenas, law enforcement databases

6.2 What methods will be used to collect the data?

Multiple methods may be used to collect information, including: 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?

OIG's process collects information from multiple sources through interviews, data requests, emails, subpoenas, law enforcement databases, and information directly from the individuals. The information received from sources is assumed to be true and accurate unless additional information obtained from other sources is contradictory. In instances where data is collected directly from the individual or entity, the individual or entity is responsible for ensuring the accuracy of the data submitted. The staff may conduct a certain degree of verification of information and follow up with an individual 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 and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

The privacy risks is that the information collected purpose and collection of the OIG-CMS data is to ensure the analysis and rendering of factual data is correctly deployed from the data of a case. OIG/OI will mitigate risk through roles and permissions, access controls, review of system logs and notifications of possible breaches such as non-OIG staff gaining access to the system or data exports (because the system will have no requirement to export data).

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.

This is a sensitive system containing law enforcement information. Individuals may not consent to the uses of the information. 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?

An individual may make a request under the Privacy Act for access to information maintained in OIG's Privacy Act system of records OIG Files, subject to certain exemptions. Individuals must follow the SEC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) 17 C.F.R. Subpart H-Regulations Pertaining to the Privacy of Individuals and Systems of Records Maintained by the Commission.

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

Yes. Individuals may request to correct or amend information about themselves in an SEC Privacy Act system of records, subject to certain exemptions. Individuals must follow the SEC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) 17 C.F.R. Subpart H-Regulations Pertaining to the Privacy of Individuals and Systems of Records Maintained by the Commission.

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

The primary privacy risk is inaccurate information maintained on individuals. This risk is mitigated by providing public notice in this PIA and the SORN of the proper procedures for individuals to request access and

amendment of their information in OIG files. Also, Additionally, the OIG collects information directly from the individual when possible. Individuals have to opportunity to provide the correct information when requested.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes
SA&A Completion Date: Click here to enter a date.
Date of Authority to Operate (ATO) Expected or Granted: 9/13/2019

☐ No
Authorization is in progress.

8.2 Identify individuals who will have access to the data in the project or system and state their respective roles.

☒ Users
Roles: Selected OIG staff to manage cases and files. This includes uploading documents and adding other case related information to cases that they have access to. Users can only access the system through a browser.

☒ Contractors
Roles: A select group of contractors may have limited access to the system for purposes of maintaining the operation of the system. The contractors will not have access to the data.

☒ Managers
Roles: Selected OIG Staff to manage cases and files

☐ Program Staff
Roles:

☒ Developers
Roles: Developers may have limited access to the system for purposes of maintaining the operation of the system. Developers will not have access to the data.

☒ System Administrators
Roles: Create, configure user accounts and the accompanying roles and permissions based on the least privilege required. The administrator can also make system wide changes to included auditing features, system timeout, and user account setting changes. All are internal OIG staff consisting of a primary and backup administrator.

☐ Others:
Roles:

8.3 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

8.4 How will the system be secured?

All OIG-CMS users are authenticated via integration with the SEC's active directory system before gaining access to the OIG-CMS. Users will also have role-based access to information in the system as determined by OIG senior staff. Roles will be assigned based on the staffer's function in the investigative workflow. Staffers not assigned to a particular case may have view only access to limited case information when necessary to carry out their official duties. For example, a staffer responsible for tracking case assignments may view the name of the case and the assigned staffer. However the staffer will not have access to the case file. OIG-CMS

administrators will monitor account activities on a regular basis. When deployed the OIG-CMS application will apply to data at rest and HTTPS during transmission sessions between end-users and the data.

Physical security controls such as guards, access through badge readers, alarms, video coverage and temperature protection of the SEC data centers will automatically be applied to OIG-CMS hosted within the SEC environment. The OIG core office is a closed environment where access is either by OIG staffers badge entry or under escort at all times. OIG-CMS will not be deployed for use to anyone outside of OIG.

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

☒ No
☐ Yes
Public
URL:

8.6 Does the site have a posted privacy notice?

☒ No
☐ Yes
☐ N/A

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

☒ No
☐ Yes, but they do not collect PII

☐ Yes, and they collect PII

8.8 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

The privacy risk identified is inadvertent or unauthorized access/disclosure of nonpublic information. However, the risk is mitigated by (1) limiting access to only OIG staffers with a need to know (2) requiring each authorized user to be authenticated prior to obtaining access; (3) utilizing granular role-based access controls (by group, user type, case type, and/or record type) to protect the data at all levels and (4) reviewing the system's audit logs on regularly for unusual activity.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

In general all staff are required to take the SEC specific privacy training and are required to comply with the OIG policy and operation

9.2 Does the system generate reports that contain information on individuals?

☐ No
☒ Yes
Investigatory Reports and Memorandums of Actions Taken are generated

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 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?

The system will log all user actions within the system. Administrators will be responsible for conducting audit reviews of the system's activities. In addition to the auditing capabilities of the OIG-CMS system, other SEC auditing tools will be utilized to generate alerts and monitor unusual activities of the system or data. See 8.4 above for additional safeguards in place.

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.

Given the sensitivity of the information collected, robust administrative, technical, and physical controls are in place to safeguard information collected by the OIG. This PIA documents the controls in the multiple sections above. Based on these controls there are no additional identified residual risks.