

Privacy Impact Assessment

Insert Project/System Name

Refer to the PIA Writer's Guide for guidance in responding to the questions below.

Contact Information

The provided contact information is for internal purposes only and will not be published to the public.

Business Owner

Name: [REDACTED]
Office/Division: Office of the Investor Advocate
Phone Number: [REDACTED]

Information System Owner

Name: [REDACTED]
Office/Division: Office of Information Technology
Phone Number: [REDACTED]

Section 1: System Overview

1.1 Name of Project or System

Ombudsman Matter Management System (OMMS)

1.2 Is the system internally or externally hosted?

- Internally Hosted (SEC) If the system is internally hosted, please list the Division or Office.
- Externally Hosted (Contractor or other agency/organization) [REDACTED]

1.3 Reason for completing PIA

- New project or system
- This is an existing system undergoing an update
- First developed: Click here to enter a date.
- Last updated: Click here to enter a date.
- Description of update: Describe the reason for the updated PIA.

1.4 Does the system or program employ any of the following technologies?

- Electronic Data Warehouse (EDW)
- Social Media
- Mobile Application (or GPS)

- [REDACTED]
- 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 Investor Advocate (OIAD) receives inquiries and complaints from the general public and responds to these communications on behalf of the Chairman. The current process of tracking and reporting complaints involves the use of manual spreadsheets which is time consuming and inefficient. The Ombudsman Matter Management System (OMMS) is a [REDACTED] which will function primarily as a case management and reporting system. The system will receive inquiries/complaints from the public and will allow OIAD to manage and keep track of the cases generated out of the inquiries/complaints. The system will also allow OIAD to generate dashboards and reports. The tool will utilize a public facing webform linked via URL redirect on the SEC.gov Ombudsman web page and a [REDACTED]. When a member of the public seeks to file a matter, they will be redirected from the SEC.gov website to

Privacy Impact Assessment

Insert Project/System Name

where they will complete an intake form.

reside on

Public users will not be required to create a user account to access or submit the matter intake web form. SEC users will have user accounts to access the Matter Management System for managing submitted matters and generating reports.

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

The applicable Privacy Act system of records (SORN) is SEC 65 and the routine uses of the records are set forth at 76 FR 30213 (May 24, 2011). This SORN is exempt from certain sections of the Privacy Act and the citation for the rule exempting the notice is 76 FR 57636 (September 16, 2011).

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:

Describe the purpose of the collection of SSNs.

Cite the specific statutory provisions or Executive Orders that authorize the collection, maintenance, use and dissemination of the data to meet an official program mission or goal.

If the data collection is part of an existing SORN, the SORN will include relevant legal authorities and should be cross referenced.

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 65

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

- No
 Yes

OMB Approval, in process.

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

Concerns of collecting publicly submitted PII were considered. This risk was mitigated in the following three ways:

- by adding a notice about PII to the top of the OMMS Submission Form: 'IMPORTANT: We do not edit personally identifiable information (PII) from submissions. To learn more about how we may use the information you send to us, please read the SEC Privacy Policy at <https://www.sec.gov/privacy.htm>.'
- by giving the public user the option to submit anonymously
- by adding following Privacy statement to the foot of the OMMS Submission Form: 'This collection of information has been reviewed by the Office of Management and Budget ("OMB") in accordance with the clearance requirements of 44 U.S.C. §3507. The applicable Privacy Act system of records (SORN) is SEC 65 and the routine uses of the records are set forth at 76 FR 30213 (May 24, 2011). This SORN is exempt from certain sections of the Privacy Act and the citation for the rule exempting the notice is 76 FR 57636

Privacy Impact Assessment

Insert Project/System Name

(September 16, 2011).'

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

- | | | |
|---|--|---|
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Alien Registration | <input type="checkbox"/> Financial Accounts |
| <input type="checkbox"/> Taxpayer ID | <input type="checkbox"/> Driver's License Number | <input type="checkbox"/> Financial Transactions |
| <input type="checkbox"/> Employee ID | <input type="checkbox"/> Passport Information | <input type="checkbox"/> Vehicle Identifiers |
| <input type="checkbox"/> File/Case ID | <input type="checkbox"/> Credit Card Number | <input type="checkbox"/> Employer ID |
| <input type="checkbox"/> Other: Click here to enter text. | | |

General Personal Data

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Marriage Records |
| <input type="checkbox"/> Maiden Name | <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Financial Information |
| <input type="checkbox"/> Alias | <input checked="" type="checkbox"/> Home Address | <input type="checkbox"/> Medical Information |
| <input type="checkbox"/> Gender | <input checked="" type="checkbox"/> Telephone Number | <input type="checkbox"/> Military Service |
| <input type="checkbox"/> Age | <input checked="" type="checkbox"/> Email Address | <input type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Race/Ethnicity | <input type="checkbox"/> Education Records | <input type="checkbox"/> Health Plan Numbers |
| <input type="checkbox"/> Civil or Criminal History | <input checked="" type="checkbox"/> Zip Code | |
| <input type="checkbox"/> Other: Click here to enter text. | | |

Work-Related Data

- | | | |
|---|--|---|
| <input type="checkbox"/> Occupation | <input checked="" type="checkbox"/> Telephone Number | <input type="checkbox"/> Salary |
| <input checked="" type="checkbox"/> Job Title | <input checked="" type="checkbox"/> Email Address | <input type="checkbox"/> Work History |
| <input type="checkbox"/> Work Address | <input type="checkbox"/> Certificate/License Number | <input checked="" type="checkbox"/> Business Associates |
| <input type="checkbox"/> PIV Card Information | <input checked="" type="checkbox"/> Fax Number | |
| <input type="checkbox"/> Other: Click here to enter text. | | |

Distinguishing Features/Biometrics

- | | | |
|---|---|--|
| <input type="checkbox"/> Fingerprints | <input type="checkbox"/> Photographs | <input type="checkbox"/> Genetic Information |
| <input type="checkbox"/> Voice Recording | <input type="checkbox"/> Video Recordings | <input type="checkbox"/> Voice Signature |
| <input type="checkbox"/> Other: Click here to enter text. | | |

System Administration/Audit Data

- | | | |
|--|--|--|
| <input type="checkbox"/> User ID | <input type="checkbox"/> Date/Time of Access | <input type="checkbox"/> ID Files Accessed |
| <input type="checkbox"/> IP Address | <input type="checkbox"/> Queries Ran | <input type="checkbox"/> Contents of Files |
| <input checked="" type="checkbox"/> Other: Date/Time of Matter submission. | | |

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

The PII collected by the OMMS is used by the OIAD Ombudsman staff to research, investigate and resolve the matters submitted by the public users. The web form submitter is give the option to submit their matter anonymously if they so choose. This removes personally identifiable fields (contact details) from the webform, but may limit the capacity to which the Ombudsman's office can assist with the submitted complaint/inquiry.

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

- SEC Employees
Purpose: [Describe the purpose of collecting the information from this source.](#)
- SEC Federal Contractors
Purpose: [Describe the purpose of collecting the information from this source.](#)

Privacy Impact Assessment

Insert Project/System Name

- Interns
Purpose: Describe the purpose of collecting the information from this source.
- Members of the Public
Purpose: The OMMS Matter intake web form is used by the public to report/submit complaints/inquiries to the Ombudsman's office and the data requested on the web form is used by the Ombudsman staff to investigate the submitted complaint/inquiry.
- Employee Family Members
Purpose: Describe the purpose of collecting the information from this source.
- Former Employees
Purpose: Describe the purpose of collecting the information from this source.
- Job Applicants
Purpose: Describe the purpose of collecting the information from this source.
- Vendors
Purpose: Describe the purpose of collecting the information from this source.
- Other:
Purpose: List other sources of information.
Purpose: Describe the purpose of collecting the information from this source.

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

The OMMS Submission Form's second question asks the public user 'Do You Wish to Report Anonymously?', if they select 'Yes' then the PII related fields (name, address, etc.) become hidden and are not required. Additionally, if the user DOES NOT report anonymously, beyond last name and an email address or phone number, all other PII related fields are not required. The PII is not being 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.
SEC has submitted all necessary documentation to NARA. The OMMS specific NARA schedule is still out for review/approval by NARA.
- Yes.
If yes, provide the retention period and cite to the NARA schedule.

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

Records are retained on the Salesforce Government Cloud until disposition is required as determined by the NARA Schedule. At that time OMMS records are downloaded/transferred to the SEC for storage on an SEC database server and/or transfer to NARA as necessary. The final business practices for these steps is an ongoing effort being developed collaboratively by SEC OIT, OIAD and the Office of Records Management.

3.7 Will the system monitor members of the public, employees, and/or contractors?

- N/A
- Members of the Public
Purpose: If the system or project monitors the members of the public, explain the purpose of the monitoring.
- Employees
Purpose: If the system or project monitors employees, explain the purpose of the monitoring.
- Contractors

Privacy Impact Assessment

Insert Project/System Name

Purpose: If the system or project monitors contractors, explain the purpose of the monitoring.

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

Considering the OMMS may potentially collect PII from public user submissions, the system was designed to be secure. Access to the OMMS back office is limited to only the SEC Ombudsman Team. All SEC users must use a unique username and password to access the system. Additionally, the OMMS has an automated timeout feature that after a set amount of time the system session closes out, combined with the SEC workstation idle timeout settings this minimizes unauthorized access to the system.

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
Link to the SEC Privacy Policy is provided in a PII disclaimer at the top of the OMMS webform.
- System of Records Notice
SORN 65
- Privacy Impact Assessment
Date of Last Update: [Click here to enter a date.](#)
- Web Privacy Policy
Where was the notice provided?
- Other notice:
What type of notice was provided? Where was the notice provided?
- Notice was not provided.
If no notice was provided, please explain why not.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

The OMMS Submission Form has a notice at the top of the form about PII and provides a link to the SEC Privacy Policy. The notice is highlighted by bold, capital letters in red font stating 'IMPORTANT'. The OMMS Submission Form also has a Privacy statement in the footer of the web page.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

OMMS does not analyze the matter record data. OIAD Ombudsman staff utilize the data to review and respond to the inquiry/complaint/matter submitted by the public user. The information is used to create a matter record. New information for an existing submitter is added to their existing record if necessary. No action is taken against individuals identified because of newly derived data.

5.2 Will internal organizations have access to the data?

- No
- Yes
Organizations: List each organization and for each organization listed describe how data is transmitted or disclosed, and the frequency of the transmissions.

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

Privacy Impact Assessment

Insert Project/System Name

N/A

5.4 Will external organizations have access to the data?

- No
 Yes

Organizations: List each organization and for each organization listed, describe how data is transmitted or disclosed, and the frequency of the transmissions.

Cite to the specific authority which allows sharing of the data.

Discuss whether the receiving system has undergone a SA&A.

For non-Federal agencies, discuss how the relevant privacy protections have been expressed and documented to ensure the privacy and security of the information once shared. State whether there is a MOU or contract or agreement in place and define parameters.

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

N/A

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): Describe the other source(s) of information.

6.2 What methods will be used to collect the data?

Public users submit information via the OMMS Submission Form.

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

Specific to the OMMS Submission Form, the Primary Email Address, Secondary Email and Email fields have format validation in place that only allows a submitter to enter data in the following format:

someone@something.com.

Specific to the OMMS [REDACTED] the Ombudsman staff are responsible for reviewing the submitted information to check for accuracy and completeness in the context of reviewing and responding to the submission.

6.4 Does the project or system process, or access, PII in any other SEC system?

- No
 Yes.

System(s): If yes, list system(s). For each listed system state the purpose of the interaction.

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?

Information provided willingly by the general public is used to respond to their matter submission in accordance with Section 919D of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. The Investor

Privacy Impact Assessment

Insert Project/System Name

Advocate appointed the Ombudsman to act as a liaison between the Commission and any retail investor in resolving problems that retail investors may have with the Commission or with a self-regulatory organization (SRO).

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.

The OMMS Submission Form is strictly voluntary. In addition public users are presented with the following three options to indicate their consent:

- By selecting 'Yes' or 'No' from the 'Do You Wish to Report Anonymously?' question.
- By selecting 'Yes' or 'No' from the 'May We Contact other U.S. Securities and Exchange Commission (SEC) Divisions/Offices, Self-Regulatory Organizations (SROs), individuals, and/or entities regarding this Matter?' question.
- By clicking the 'Cancel' button at the bottom of the page, which removes all content from the form and returns the user to the www.sec.gov/ombudsman webpage.

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

All information regarding an individual is supplied by the individual either via the OMMS Submission Form or as provided to an Ombudsman Staff Member. Public submitters do not have direct access to the Matter record created from their submission. If a public user wishes to inquiry about their submission or provide updated information they can contact the SEC Ombudsman's Office by phone, email or mail.

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

Public submitters cannot directly alter/update information they provided on the OMMS Submission Form after they click the Submit Form button. If a public user wishes to provide update information they can either submit a new intake form OR contact the SEC Ombudsman's Office by phone, email or mail.

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

The OMMS Submission Form is voluntary. If they decide to submit the form, the user has the option to limit the information they submit, either by selecting to report anonymously or entering the minimally required fields.

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: [Click here to enter a date.](#)

No

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

Users

Roles: [Click here to enter text.](#)

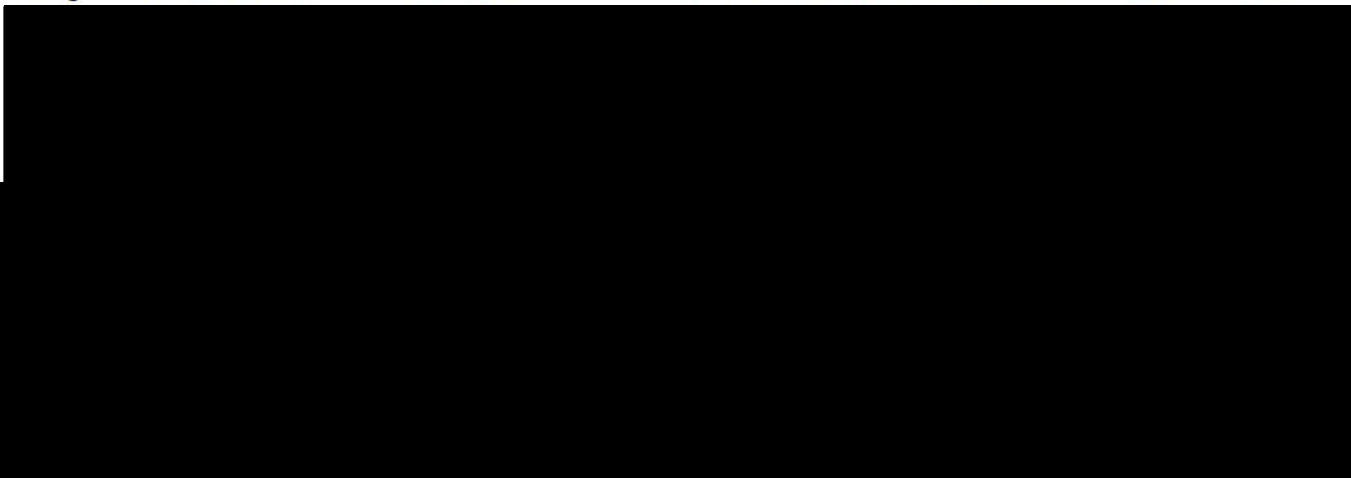
Contractors

Roles: [Click here to enter text.](#)

Privacy Impact Assessment

Insert Project/System Name

- Managers
Roles: [Click here to enter text.](#)
- Program Staff





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

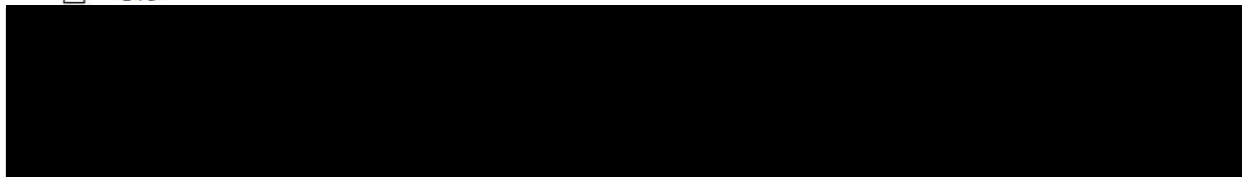
8.4 How will the system be secured?

OMMS Submission Form – public-facing does not require login or authentication and is accessed via URL/web-browser. Only for use by the public.

OMMS  SEC users access the  via URL and require a unique username and password to login. 2-factor authentication is used. All passwords are encrypted in storage and transmission.

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

- No



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



Privacy Impact Assessment

Insert Project/System Name

- Yes, and they collect PII

List the types of web measurement or customization technologies used, e.g., web beacons, web bugs, session cookies, persistent cookies, etc. and the types of PII they collect.

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.

PII information submitted by the public via the OMMS Submission Form is only used to review and respond to their submission. ██████████ DMMS ██████████ back office requires SEC users to use 2-factor authentication, username and password to access the system.

Section 9: Accountability and Auditing

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

Public Users: To learn more about how we may use the information you send to us, please read the SEC Privacy Policy at <https://www.sec.gov/privacy.htm>. (notification on top of OMMS Submission Form.)

SEC Users: All SEC employees are required to complete ██████████ training on PII.

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

- No
 Yes

If yes, describe how the reports or data extracts are secured. Describe the retention and disposal procedures for the data extracts or reports.

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

Audit logs are created/maintained for all System Administrator actions and the following three fields are tracked for changes: Status, File Owner and Anonymous (Y/N). Audit records are maintained by ██████████ for 18 months. At or before 18 months, SEC must employ a manual process to download the audit records ██████████ and store them on SEC database infrastructure.

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?

To prevent misuse of data there are three aspects of security that ██████████ has implemented. The first aspect is *users and security*, looking at how users are authenticated, network-based security that determines the IP ranges

Privacy Impact Assessment

Insert Project/System Name

from which a user may access the network, sessions and auditing.

The second aspect is *programmatic security*. Any software client that needs to log in to the platform [REDACTED]

The third aspect is the [REDACTED] *platform security framework*, which you can use to offer different access permissions to authenticated users within your organization. This security framework lets you grant security permissions to users or profiles, determine access control over a wide range of components (such as tabs or persistent objects), and configure data sharing, which limits access to individual records. Some of this security framework is administrative (only allow these user profiles access to this application), while some is also relevant to your application architecture (ensure that these records are always visible to managers).

At an infrastructure and network level, [REDACTED] applies rigorous security standards, such as [REDACTED]. Another corporate site of interest is [REDACTED] which provides real-time information on system performance and security, including information on security alerts.

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.

Expected residual risk for PII in the system is minimal.

Individual Completing this Form

Name:

Date:

7/13/2016

Email: