U.S. Securities and Exchange Commission

Ombudsman Matter Management System (OMMS)
PRIVACY IMPACT ASSESSMENT (PIA)

September 15, 2016

Office of the Investor Advocate

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)

☒ Externally Hosted (Contractor or other agency/organization) Salesforce Solution developed by Acumen

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
☒ 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) Ombudsman receives inquiries and complaints from members of the public (submitters) and responds to these communications on behalf of the Chairman. The Ombudsman Matter Management System (OMMS) will function as a case management and reporting system that will allow the Ombudsman to receive inquiries or complaints from submitters and automate the tracking of the cases generated out of those inquiries or complaints. The system will also allow the Ombudsman to generate dashboards and reports. Typical reports generated by the system include:

- The number of inquiry/complaint submissions
- The number of matters by age, status, or submission date
- The number of matters by inquiry or submission type, and/or
- The number of matters by city, state, or region

Submitters complete an intake form on an OMMS webpage to submit an inquiry or complaint. They may attach related documents relevant to their inquiry/complaint. Submitters have the option of providing personally identifiable information (PII) such as name, address, etc. as contact information, or making an anonymous inquiry/complaint. For anonymous submissions, when a submitter elects to submit anonymously, PII-related data fields on the intake form will become unavailable. When a submitter submits a complaint/inquiry on the OMMS web browser they are redirected from the SEC.gov website to Force.com, which resides on the Salesforce cloud platform. Any documents attached are stored in the Salesforce database. Submitting an inquiry or complaint is completely voluntary. However, if the submitter wants the

Ombudsman to follow-up with them, they will have to provide some contact information.

Ombudsman staff will be able to access the submissions internally via a secure web browser from within the SEC environment. The Ombudsman will be able to review the information provided and assign matters in the queue to the appropriate staff.

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

Section 919D of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010**.**

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:

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- 29, "Agency Correspondence Tracking System (ACTS)"

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?

The privacy risks associated with the purpose of the collection is the collection of more information than necessary. Submitters are allowed to upload documents to support their inquiry/complaint which will become a part of the matter record. To mitigate the collection of information that the SEC does not request, notice is provided on the OMMS intake form which notifies individuals that personally identifiable information is not edited from submissions. Submitters are requested to submit only the information relevant to the matter. Individuals are also provided a link to the SEC's privacy policy which puts them on notice that voluntarily providing information to the SEC acts as consent to the SEC's use of that information and permits that information to be shared with SEC employees and contractors and, in limited circumstances, with third parties, to conduct official business.

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
☐ Taxpayer ID
☐ Employee ID
☐ File/Case ID
☐ Alien Registration
☐ Driver's License Number
☐ Passport Information
☐ Credit Card Number
☐ Financial Accounts
☐ Financial Transactions
☐ Vehicle Identifiers
☐ Employer ID

☐ Other:

General Personal Data

☒ Name
☐ Maiden Name
☐ Alias
☐ Gender
☐ Age
☐ Race/Ethnicity
☐ Civil or Criminal History
☐ Other:

☐ Date of Birth
☐ Place of Birth
☒ Home Address
☒ Telephone Number
☒ Email Address
☐ Education Records
☒ Zip Code

☐ Marriage Records
☐ Financial Information
☐ Medical Information
☐ Military Service
☐ Mother's Maiden Name
☐ Health Plan Numbers

Work-Related Data

☐ Occupation
☒ Job Title
☐ Work Address
☐ PIV Card Information
☐ Other:

☒ Telephone Number
☒ Email Address
☐ Certificate/License Number
☒ Fax Number

☐ Salary
☐ Work History
☒ Business Associates

Distinguishing Features/Biometrics

☐ Fingerprints
☐ Voice Recording
☐ Other:

☐ Photographs
☐ Video Recordings

☐ Genetic Information
☐ Voice Signature

System Administration/Audit Data

☐ User ID
☐ IP Address
☒ Other: Date/Time of Matter submission.

☐ Date/Time of Access
☐ Queries Ran

☐ ID Files Accessed
☐ Contents of Files

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

OMMS collects PII submitted primarily as contact information by submitters of inquiries or complaints. The PII collected allows the Ombudsman staff to track, research, investigate and respond to the inquiries or complaints. Additionally the Ombudsman uses the information to facilitate the processing of complaints and inquiries, to include maintaining a record of the submission and forwarding the correspondence to the proper office for action internally.

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

☐ SEC Employees
Purpose:
☐ SEC Federal Contractors
Purpose:
☐ Interns
Purpose:
☒ Members of the Public
Purpose: The OMMS Submission intake web form is used by the public to submit complaints/inquiries to the Ombudsman. The data requested on the web form is used by the staff to investigate the submitted complaint/inquiry.
☐ Employee Family Members
Purpose:
☐ Former Employees
Purpose:

☐ Job Applicants
Purpose:
☐ Vendors
Purpose:
☐ 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.

The OMMS Submission Form minimizes the collection of PII by allowing users to submit an inquiry or complaint anonymously. If a submitter decides to report anonymously, fields that contain PII (name, address, etc.) become hidden and are not required. If the user does not report anonymously, a last name and an email address or phone number, are the only PII data elements required. Any PII collected or maintained in OMMS 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.
A records retention schedule is under review by NARA. Until the schedule has been approved, records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with record schedules of the SEC.
☐ Yes.

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 Platform until disposition is required as determined by the NARA Schedule. At that time OMMS records are downloaded and transferred to the SEC for storage on an SEC database server and/or transferred to NARA as necessary. The final business practices for these steps are an ongoing effort being developed collaboratively by the SEC Office of Information Technology (OIT), OIAD Ombudsman 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:
☐ Employees
Purpose:
☐ Contractors
Purpose:

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

Unauthorized disclosure or unauthorized access is the primary risk to the type of information collected. To mitigate these risks, the SEC requires the completion of appropriate access agreements for individuals requiring access to information systems before authorizing access. Additionally, there are role-based access controls within OMMS which limits access to selected groups for prescribed functions. All employees with access to the system are required to take security and privacy awareness training on an annual basis.

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- 29, "Agency Correspondence Tracking System (ACTS)"
☐ Privacy Impact Assessment
Date of Last Update:
☒ Web Privacy Policy
A link to the SEC's Web Privacy Policy will be provided on the intake form.
☒ Other notice: Upon finalization of this PIA, this document will provide notice of the administrative, technical, and physical controls protecting this information.

☐ 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 identified is inadequate notice to individuals of the information OMMS will collect, how it will be used, and the technical, physical and administrative controls surrounding the data. Publication of this PIA will provide a detailed description of what information OMMS will collect, use, and disseminate and will assist individuals in fully understanding the system. Additionally, on the intake form, individuals are provided a link to the SEC's Web Privacy Policy. This Privacy Policy describes the SEC's uses of personal information. The SORN, PIA, and Web Privacy Policy combined provide adequate notice.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

OMMS does not analyze PII collected nor will it be used to derive new information. The primary purpose of this system is to support the resolution of public inquiries or complaints. While metrics may be used in support of work efforts, data mining is not within the scope of this system.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: Other offices/divisions will not have direct access to OMMS, but may be made aware of correspondence contained within the system to assist in resolving an inquiry or complaint. Information will be shared only with divisions and offices as appropriate to determine and develop options for resolution to the inquiry/complaint.

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

Privacy risks associated with internal sharing are unauthorized access or unauthorized disclosure of an inquiry/complaint and unauthorized use of information. Ombudsman staff has role-based access to OMMS. These access controls are based on those with a valid need to know. Other offices/divisions will not have direct login access to OMMS, but may be made aware of information contained within the system to assist in resolving and inquiry or complaint. Information will be shared only on a need to know basis.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes
Organizations: The Salesforce system administrator will have system-level privileges (i.e. security settings, field settings, OMMS user account management, etc.). Only the Ombudsman and staff have user-level privileges (i.e. the ability to create, edit, delete matter records or matter submitter accounts, etc.).

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

To mitigate an inadvertent release of PII, other information systems do not have direct access to OMMS. Other agencies or external vendors will not have access to OMMS. Information collected in OMMS may be shared with an external organization only if the Ombudsman is authorized to disclose the 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):

6.2 What methods will be used to collect the data?

Submitters submit their information via the OMMS intake form and any uploaded attachments. Once a user completes the intake from and clicks the submit button, the case record along with any uploaded document(s) are saved in OMMS's repository.

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

Information is collected directly from individuals. The Ombudsman relies on this information and the correspondence is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise. Additionally, the OMMS Submission Form has data integrity checks built into the system; the email fields have format validation in place that only allows a submitter to enter data in a specific formation (i.e. someone@something.com). Ombudsman staff reviews all submissions to verify that information provided is sufficient to respond to an inquiry or complaint.

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?

Privacy risks related to data quality and integrity are minimal. Data is primarily collected voluntarily from submitters submitting the inquiry/complaint. Also, individuals are allowed to make submissions anomalously without disclosing any PII. The methods for submitting requests mitigate the privacy risks associated with OMMS collection of information. Additionally, SEC staff review the submitted information to ensure that enough information is provided to effectively respond to the inquiry or compliant.

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.

When submitting an inquiry/complaint, individuals may decline to provide PII or limit the PII provided. Making a submission is completely voluntary. However, once information is presented, submitters do not have the opportunity to consent to particular uses of the information.

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 intake form or as provided to Ombudsman staff member. Submitters do not have access to the information they submit after completing the submission. If they wish to inquire about their submission or provide updated information they can contact the Ombudsman by phone, email or mail. They also may submit a Privacy Act request or Freedom of Information Act (FOIA) request.

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

Submitters cannot directly alter/update information they provide on the OMMS intake form after they click the submit form button. If a public user wishes to provide updated information they can either submit a new intake form or follow the procedures in 7.2 above.

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

Privacy risks related to individual participation and redress are minimal in OMMS. Individuals voluntarily submit any PII collected in the system and have the option to make anonymous submissions. The various methods of notice are provided to the individual to caution individuals from including more information than is needed..

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
The SA&A is currently underway and is anticipated to be complete by 9/20/16.

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

☒ Users
Roles: Members of the public who submit inquiries/complaints
☐ Contractors
Roles:
☒ Managers
Roles: Managers can reassign matters in the queue to individual users in OIAD to be worked.
☒ Program Staff
Roles: Ombudsman staff have several roles with slightly varied privileges:
Ombudsman: Can read, write, edit, and delete records.

Senior Counsel Ombudsman Operations: Can read, write, and edit records.
OIAD Team: Can read, write, and edit records.
Interns: Can read records (read only).

☒ Developers
Roles: Can access system to make system, field and settings updates as needed.

☒ System Administrators
Roles: Can modify settings and update fields, add, modify and disable user accounts.

☐ 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?

The OMMS has two main components – 1) the public-facing OMMS Submission Form and secure web browser; and 2) the OMMS secure internal web browser which is only used by SEC Ombudsman staff users.

The OMMS Submission Form does not require public users to use any authentication or login.

The OMMS internal system is only used by internal SEC Ombudsman staff. Ombudsman staff must use a uniquely assigned username and personalized password to log into the Salesforce platform. Security options have been enabled that require a user accessing OMMS to do so from within the SEC's network. Even, internal users with an OMMS account cannot access the system without accessing it via the SEC network. The Ombudsman authorizes new users, user privileges, privilege changes and user account freezes.

Only Salesforce employees with two-factor authentication and role-based access to the Salesforce network. Submitters and the SEC staff utilize a secure connection from their applicable browser to OMMS. Kerberos is also used to prevent Salesforce employees from using any unauthorized application, including those that might allow connecting to the Internet or scraping customer data. Individual user sessions are identified and re-verified with each transaction, using a unique token created at login.

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

☐ No
☒ Yes
Public URL: https://secir.my.salesforce.com/ombudsman/OMMSForm

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

Salesforce.com provides each user with a unique username and password that must be entered each time a user logs in. Salesforce.com issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include either the username or password of the user. Salesforce does not use cookies to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

☐ 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.

OMMS provides users with an option to upload an attachment to support their inquiry or complaint. This presents a possibility that a user could upload a malicious file and compromise the security of the database. If a virus or infected file is uploaded from an external user, controls are implemented so the file will not damage or compromise the salesforce services. Any damage would be limited to an internal user's local machine and that is only if the infected attachment is opened or downloaded. At the SEC, users have antivirus software on their workstations which protect SEC workstations from damage from malicious files.

Additionally, there is a risk that malicious or inadvertent actions taken on a particular correspondence may not be traceable back to an individual. This risk is mitigated within OMMS by auditing controls whereby actions taken by a user are tracked. A six month history of all login attempts to the organization, including username, IP addresses, success/failure, and time and date is available from Salesforce on request and a 180-day history of setup changes made by the SEC's administrators is also available upon demand, and can be used to troubleshoot and audit administrative activities.

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 personnel are required to take annual privacy and security training which outline their roles responsibilities in handling PII. Additionally, Salesforce's employees who are engaged in the processing of personal data have executed written confidentiality agreements and have received appropriate training on their responsibilities.

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

Audit logs are created and maintained for all System Administrator actions. Audit records are maintained by Salesforce for 18 months. At or before 18 months, SEC must employ a manual process to download the audit records from Salesforce and store them on SEC database infrastructure. Failed login attempts, changes to user groups or system accounts, and password changes are all tracked.

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?

Salesforce has embedded auditing capabilities within the application and are responsible for auditing at the platform level. Salesforce Administrators are responsible for reviewing and analyzing the system specific Force.com platform audit records, including: the Setup Audit Trail, Login History, and Object History reports. The audit records are reviewed on a weekly basis for indications of inappropriate or unusual activity and for reporting findings to designated organizational officials (System Owner/SEC OIT Security Ops). Administrators are also responsible for adjusting the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, and/or individuals based on law enforcement information, intelligence information or other credible sources of information.

The Salesforce platform produces audit records for agency users that contain information at a minimum to establish what type of event occurred, when (date and time) the event occurred. Where the even occurred is identified as either OMMS Submission Form or OMMS back office. Where the event occurred, the outcome (success or failure) of the event, and the identity of any individuals/subjects associated with the event are not tracked at this time.

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.

There is a risk of an authorized user having more permissions than required to perform their job function. This risk exists when any user account is created. To mitigate this risk, the Ombudsman is responsible for identifying the account types utilized in the OMMS. Individual users are only granted the permission that they are authorized to hold and for which they have an authorized need. The system maintains a list of all approved users and accounts. The SEC designated representative informs the System Administrator who then designates the appropriate privileges to be assigned to new accounts based on the specific role. The SEC representative or designated System Administrator reviews the list of active accounts on the system bi-annually.

To mitigate the risk of an unauthorized SEC employee from viewing material in OMMS, OMMS has session locks and process termination routines. OMMS automatically terminates inactive sessions within a SEC mandated time-out period of inactivity. After a session is terminated, the OMMS user must re-establish the session using the appropriate identification and authentication procedures. Accounts are locked after five consecutive invalid login attempts over any time period. The period of lockout is set to 15 minutes.