U.S. Securities and Exchange Commission

Office of the Chief Accountant
PRIVACY IMPACT ASSESSMENT (PIA)

September 13, 2013

Privacy Impact Assessment
Office of the Chief Accountant (OCA)

General Information

1. Name of Project or System.
   Office of the Chief Accountant - Accounting

2. Describe the project and its purpose or function in the SEC's IT environment.
   The Office of the Chief Accountant – Accounting application ("OCA") is used to assign work to the Accounting Group staff, to record the status of the issues assigned, and to maintain documents relevant to each assignment. OCA categorizes issues based on subject areas determined by supervisors. In combination with the appropriate access controls and preferences, it allows users to access what is relevant to their function or particular task. It allows supervisors to create issues by type (consultation, standard-setting, rulemaking, etc.). The supervisors can then assign the newly created issues to staff members specifying a team lead. The assignees are able to enter their inbox and see the open issues assigned to them. Also, they are able to update information relevant to the given issue. This can include general information about the issue, notes and documents associated with an issue. The users can also create correspondence, speech and/or meeting logs and associate those to a particular issue. As set forth in greater detail in Section I, Question 1, below, the system may collect and maintain names, mailing addresses, telephone numbers and email addresses of various external individuals. The system also maintains names of internal employees assigned to any given issue.

3. Requested Operational Date? OCA has been operational since 12/2007. The most recent recertification for the system occurred in February 2011. This PIA is being conducted to assess the current privacy risks and vulnerabilities of the data collected.

4. System of Records Notice (SORN) number? SEC-28, Office of Chief Accountant Working 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? 15 U.S.C. 77a et seq. 78a et seq., 7201 et seq. and 17 CFR 200.22

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   Employee names. Correspondence from external parties is uploaded to the system and attached to an issue. Such correspondence may include names, mailing addresses, telephone numbers, and email addresses of various external individuals, including employees of issuers, their external accountants, or legal counsel.

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.

3. What are the sources of the data?
   Employee names are drawn from the payroll system. External data typically comes from employees of issuers, their external accountants, or legal counsel.

4. Why is the data being collected?
   Employee names are associated with issues to track who is assigned to each issue. Correspondence from external parties, which may contain PII, is retained for knowledge retention purposes and to maintain a full record of the issue.

5. What technologies will be used to collect the data?
   Email, scanning (for submissions made via hardcopy or fax)

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

1. Describe the uses of the data.
   Employee names are used to associate issues with the employees assigned to work on them. We use the contact data included in the correspondence to communicate with the external parties. Names or other personal information, generally limited to the types described in Section I, Question 1, may also be present in the body of submissions and may be used in the consultation process.

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:

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   PII is not checked for accuracy.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☐ No ☒ Yes If yes, please list organization(s): Individuals in the Division of Corporation Finance's Office of Chief Accountant have access to OCA. As appropriate, information may be shared with other divisions within the SEC.

2. Will the data be shared with any external organizations?
   ☒ No ☐ Yes If yes, please list organizations(s):
   How is the data transmitted or disclosed to external organization(s)?
3. How is the shared data secured by external recipients? N/A

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

SECTION IV - Notice to Individuals to Decline/Consent Use

1. What privacy notice was 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 was not provided to individuals prior to collection

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☒ Yes ☐ No ☐ N/A
   Please explain: Correspondence to The Office of the Chief Accountant that is maintained in OCA is voluntary.

3. Do individuals have the right to consent to particular uses of the data?
   ☐ Yes ☒ No ☐ N/A
   Please explain: Once correspondence from external parties is provided the information will be used for purposes compatible for which it was collected. Employees may not request that we not track the issues to which they are assigned.

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?
   SEC staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII.

3. Has a system security plan been completed for the information system(s) supporting the project?
   ☒ Yes If yes, please provide date C&A was completed: 2/2011
   ☐ No If the project does not trigger the C&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 (ie. periodic, recurring, etc.) PII data extractions from the system?
   ☒ No
   ☐ Yes If yes, please explain:

6. Which user group(s) will have access to the system?
   There are four levels within OCA: Application User, Accounting User, Accounting Supervisor, and Administrator . Employees with access may be members of the Office of the Chief Accountant or the Division of Corporation Finance.

7. How is access to the data by a user determined? The use of OCA is strictly limited to authorized SEC users designated by the Office of the Chief Accountant.

   Are procedures documented? ☒ Yes ☐ No

8. How are the actual assignments of roles and rules verified.
   Annual access review.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data? Auditing measures/controls and technical safeguards include user account identification and authentication, role based access, and SSL connection to the application.

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 associated with the collection of the data include potential release to unauthorized users of the data identified in Section I. The staff views the risks associated with release as low. Any privacy concerns are mitigated by strictly limiting access to OCA by Office of the Chief Accountant and Division of Corporation Finance employees with a need to know. Access controls are implemented on production systems through the use of system usernames and passwords as well as database (application) usernames and passwords.