U.S. Securities and Exchange Commission

External Application User Administration (EAUA)
PRIVACY IMPACT ASSESSMENT (PIA)

September 30, 2013

Privacy Impact Assessment
External Application User Administration (EAUA)

General Information

1. Name of Project or System.
   External Application User Administration (EAUA)

2. Describe the project and its purpose or function in the SEC's IT environment.
   The U.S. Securities and Exchange Commission (SEC) has been deploying an increasing number of applications accessible by non-SEC users via the Internet. In order to more easily manage the large volume of user accounts associated with these external applications, the External Application User Administration (EAUA) system has been developed. EAUA enables potential users of external applications to request accounts for new users, as well as enable access to additional applications for existing users; gives SEC personnel the ability to review these account / application access requests and, upon approval, create the accounts automatically. The entire process is done electronically. The purpose of EAUA is to track and easily manage the large volume of user accounts associated with external applications.

   The following list of applications use EAUA for user authentication:
   - Testimony Tracking System (TTS-vendor)
   - SRO Referral System (SIRS)
   - Municipal Advisor Temporary Registration (MATR)
   - Electronic Form 19b-4 Filing System (EFFS)
   - Broker-Dealer Risk Assessment (BDRA)
   - Bluesheet Direct Submission (BLUEXT)
   - Rule 19d-1 (Rule19d-1)
   - NRSRO-ETR

3. Requested Operational Date? EAUA originally became operational in mid-2003 and was first certified in 2007. Recertification activities were conducted in December 2010 and January 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? N/A. The data is not retrieved using a personal identifier of an individual. The Search Accounts function allows retrieval of information by Organization Name, User Name (derived from company email address), Start Date, End Date, Account Status and Application Status. SORNs are published for those applications accessible via EAUA, as applicable.

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? 5 U.S.C. 302.

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   The EAUA Approval Form collects the following information from the applicant: Applicant's First and Last Name, Company Email, Company Mailing Address, Company

Phone Number and Company EIN, Name, Mother's maiden name, user-id. In some cases this is personal email and personal telephone number, thereby changing what kind of data this application collects.

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?
   A SEC user logs into an EAUA-enabled internal Web App and sends an external user a link to the EAUA-Request Application or to the EAUA-User application if they are an existing user (this is one of the EAUA Account Management Features.) The external user uses this link to submit information required for account creation to the EAUA Request Web App or to request access to another application if they are an existing user. (Alternatively, an SEC user may request an account on behalf of the external user.)

4. Why is the data being collected?
   Data is collected to verify the non-SEC users/applicant's identity and verify if the applicant has a bona fide need to access an external SEC web application.

5. What technologies will be used to collect the data?
   Data entered on the application form will be stored in a database. EAUA is a Web application that has an internal component for SEC users and an external component for non-SEC users. Digital certificate may be used to issue or reject new account requests. This creates a tamper-proof way of maintaining an audit trail of EAUA account approvals.

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

1. Describe the uses of the data.
   - Applicant's First and Last Name – To identify the person that is requesting access to the application
   - Applicant's work email address – The email address where the application link will be sent. This is sometimes a personal email address.
   - Company Name – To identify the company where the applicant works and used to verify the name on file with EDGAR
   - Company's EIN – To identify the company's Employer Identity Number
   - Company's Mailing Address
   - Company's EDGAR CIK No – Used to search EDGAR filings
   - Telephone number – To identify the company's telephone number

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?

There are different administrators for different applications. The assigned system administrator for the application will verify the data provided in the EAUA form.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☒ No ☐ Yes If yes, please list organization(s):

2. Will the data be shared with any external organizations?
   ☒ No ☐ Yes If yes, please list organizations(s): The only information that the external recipients have access to is the data they entered. In order to access it they must login (using SSL) to the external system with their personal account.

   How is the data transmitted or disclosed to external organization(s)? The only information that the external recipients have access to is the data they entered. In order to access it they must login (using SSL) to the external system with their personal account.

3. How is the shared data secured by external recipients?
   The only information that the external recipient has access to is the information originally submitted. The recipient is responsible for the manner of securing the information provided.

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

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: Applicants may decline to complete the request for an account form. However if the applicant declines providing the information requested it could result in their request for access to EAUA being denied.

3. Do individuals have the right to consent to particular uses of the data?
   ☐ Yes ☒ No ☐ N/A
   Please explain: Once the Applicant provides the information requested in the application the information will be used for purposes compatible for which it was collected, i.e., provide access to the applicable application.

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: February 22, 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?
   - The "EauaAdmin_role" role is required to search accounts, as well as specific designation as an admin for a given application (multiple applications allowed). Searches for accounts by Administrator only pulls back Accounts that have access to applications of which the given user is an admin.
   - "EauaApprove_role" is required for 1st level approval of accounts; this also requires specific designation for a given application as a 1st level approver. This approver is supposed to verify the applicants need for an account and their account information. They make the initial association for the account with whatever registered entity is represented (i.e., Broker/Dealer or SRO).
   - "EauaApprove_role" is required for second tier approval of accounts; this also requires specific designation for a given application as a 2nd level approver. This approver is typically the supervisor or application owner of this application. This is to ensure that they are aware of who is requesting accounts.
   - "EauaSecurity_role" is a role for OIT security to access the system to approve accounts. It was originally designed for a third tier of approval but after EAUA went to production, OIT Security decided they did not want to approve all accounts. The role is still available in the system.

7. How is access to the data by a user determined? The Business Owners request the roles, the System Owners approve the roles, and the Database Administrators implement the roles.
   Are procedures documented? ☒ Yes ☐ No

8. How are the actual assignments of roles and rules verified.
   The Business Owners request the roles, the System Owners approve the roles, and the Database Administrators implement the roles.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
   Application-specific audit information and functions have not been formally defined and documented for EAUA. No procedures are in place to ensure that application audit logs are regularly reviewed to ensure timely detection of malicious activity.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

A few of the privacy risks associated with this system include the following:

- There is no way to monitor who should be made inactive.
- There seems to be no way for anyone to check to see if they have an account, so duplicates are prevalent.
- There is no way to uniquely identify a person.
- Invalid email addresses are being used for SEC employees.
- Personal email addresses are being used.
- Reuse of passwords for external users of applications supported by EAUA is not prevented.

To mitigate some of these issues, EAUA has a number of security protections, such as automatic expiration of unused accounts, locked accounts for excessive invalid login attempts, and email validation of account activations and forgotten password requests. In addition, the database design follows the standard auditing requirements put forth by the Data Architecture Working Group at the time this application was developed. For example, it records the employee ID of the creator of any account as well as the last person to modify an account. It also records who approved the account, storing their digitally signed approval (which is required for approval of all accounts).