U.S. Securities and Exchange Commission

SRO Rule Tracking System/Electronic Form Filing System (SRTS/EFFS) PRIVACY IMPACT ASSESSMENT (PIA)

September 30, 2013

Division of Trading and Markets

Privacy Impact Assessment
SRO Rule Tracking System (SRTS)/Electronic Form Filing System (EFFS)

Contact Information

System Owner Name: [redacted], Sr. Accountant
Office/Division: Trading and Markets Telephone Number: [redacted]

Project Manager Name: [redacted]
Office/Division: OIT/DIO Telephone Number: [redacted]

General Information

1. Name of Project or System.
   SRO Rule Tracking System (SRTS)/ Electronic Form Filing System (EFFS)

2. Describe the project and its purpose or function in the SEC's IT environment.
   SRTS/EFFS is a secure, web-based E-filing application that allows Self-Regulatory Organizations (SRO) to file proposed changes to their rules with the Securities and Exchange Commission (SEC) for notice, public comment, and Commission approval prior to implementation. SROs also use the external application component (EFFS) to submit filings and pre-filings for non-controversial filings and SEC personnel are able to receive, act, and respond to them electronically using the internal component (SRTS). SRTS/EFFS allows the Division of Trading and Markets to record and track the status of Form 19b-4 filings submitted by SROs.

3. Requested Operational Date? SRTS originally became operational in 2002, while EFFS became operational in 2004. A Security Risk Assessment was conducted in April 2008 and May 2010. Mini v4 assessment was conducted in November 2010. Major v5 release is scheduled for December 2013. This PIA documents the privacy risks and vulnerabilities of the data collected.

4. System of Records Notice (SORN) number? A SORN is not required for this system since the data is routinely retrieved by the filing number.

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? The Securities Exchange Act of 1934

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   SRTS collects information from Form 19b-4 which has the name, phone number, fax number and e-mail address of the attorney who filed the filing.

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?
   SROs who are required to complete Forms 19b-4.

4. Why is the data being collected?
   Form 19b-4 data are collected to respond to questions and comment on the proposed rule changes, advance notice filings and security-based swap submissions.

5. What technologies will be used to collect the data?
   Data are collected by the IBM Forms Viewer and Java JSP web form with the https connection, which provides encrypted communication and secure identification of a network web server.

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

1. Describe the uses of the data.
   SRTS collects information from Form 19b-4, which has the name, phone number, fax number and e-mail address of the attorney who filed the filing. This data is used to contact the attorney who provided the form on matters related to the review and approval process for SRO rule changes that could affect stock markets and investors.

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?
   The data collected is that entered by the filer. The Filer is required to provide accurate, and clear information pursuant to the legal authorities identified above. Data entered by SEC staff is verified through various internal controls, policies and procedures.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☐ No ☒ Yes If yes, please list organization(s): The application is owned by the Division of Trading and Markets (TM), and the user base consists of authorized TM, Office of the Secretary (OS), and Office of Compliance, Inspections, and Examinations (OCIE) staff and various SRO personnel, as well as other Commission Divisions and Offices, as needed.

2. Will the data be shared with any external organizations?
   ☐ No ☒ Yes If yes, please list organizations(s): The data may be shared with Congress and GAO. The shared data are public, non-PII data.

   How is the data transmitted or disclosed to external organization(s)? Data is generally extracted and provided via PDF or Excel spreadsheet reports.

3. How is the shared data secured by external recipients?
   The shared data are public, non-PII data and are such, not subject to any special security requirements.

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

   Please explain: In order to file Form 19b-4 through EFFS, SROs must request access to the SEC's External Application Server or (EAUA, External Application User Administration) by completing a request for an external account user ID and password. The EAUA web-form contains a link to the SEC's Web-Privacy Policy.

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☐ Yes ☒ No ☐ N/A
   Please explain:
   The filers are required to file the information pursuant to the federal security laws.

3. Do individuals have the right to consent to particular uses of the data?
   ☐ Yes ☒ No ☐ N/A
   Please explain:

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:
   These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with records schedules of the United States Securities and Exchange Commission as 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?
   All 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: April 4, 2008. Production for major v5 release scheduled for December 27, 2013. SA&A documents due December 13, 2013.
   ☐ 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?
Only SEC staff with the authorized login can access the system. The type of access is limited by user's roles.

7. How is access to the data by a user determined?
SRTS use following roles to assign privileges to users:
Authorized TM staff will be assigned one or more of the following roles in SRTS:
   - Administrator - Super-user access
   - Gatekeeper - New 19b-4 filings/pre-filings are received in the Gatekeeper Inbox. The Gatekeeper reviews the rule filing and assigns it to an AD/SSC.
   - 19b7Gatekeeper - New 19b-7 filings are received in the 19b7Gatekeeper Inbox. The gatekeeper reviews the rule filing and assigns it to an AD/SSC.
   - AD/SSC - New and open filings and pre-filings assigned to an AD/SSC are displayed in the AD/SSC Inbox. AD/SSC reviews the rule filing and assigns it to a Principal Attorney and Staff Attorney(s). AD/SSC can change the status of pre-filings to Acceptable or Unacceptable. AD/SSC can run the AD/SSC Open Report, Office Open Report, and Workload Summary Report.
   - Attorney - New and open filings and pre-filings assigned to an attorney are displayed in the Attorney Inbox. Attorneys can update Docket information as they process and review rule filings. Attorneys can run the Attorney Open Report, Office Open Report, and Workload Summary Report.
   - Secretary - New and open filings assigned to a secretary are displayed in the Secretary Inbox. The Secretary Inbox will also display the following conditions that may apply to a filing: Withdrawal, Rejection, Closed, New Amendment, and New Extension. Secretary can update all data. Secretary can run the Office Open Report and Workload Summary Report.
   - Associate Director – Open filings assigned to an Associate Director are displayed in the Associate Director Inbox. Associate Director can run the Associate Director Open Report, Office Open Report, and Workload Summary Report.
   - External SROs only have one type of account for submitting filings through EFFS.

   Are procedures documented? ☒ Yes ☐ No

8. How are the actual assignments of roles and rules verified.
Supervisors submit a request to the Division's IT staff, who subsequently submit the request via the ITSM system. System Administrators review the access and either approve/ disapprove the access request.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
   All of the information in the data is available for any authorized users. Only authorized users have access to the system (i.e., it is only accessible via the Insider). The documents submitted are publicly available as well.

SECTION VI - Privacy Analysis

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

The scope of the personal information collected is limited to the amount of data necessary to act upon requests, correspondence, or other possible action items received related to SRO filings and pre-filings.

The SEC has implemented user access controls requiring positive user identification (ID) and authentication. Each user account requires a two-step process, an entry within the application by the system owner and within the corresponding Sybase or MySQL database by GSS staff.

SRTS/EFFS enforces good segregation of internal and external functions. Non-SEC users only access the EFFS component of the system, which resides in the DMZ.

All data is transferred via orderly and secure processes. The SRTS/EFFS Sybase and MySQL databases provide a suite of audit reports that are run periodically and reviewed according to established procedures.

Access to the security functions (e.g., audit trails, access control lists, and password files) is restricted to system administrators, database administrators, and the information system security officer (ISSO). All activity associated with these user groups is recorded in the audit trail.

Person completing this form

Name: [redacted] Telephone Number:x[redacted]