Privacy Impact Assessment
Tips, Complaints, and Referrals (TCR) Intake and Resolution System

CONTACT INFORMATION

1. System Owner Name, Title, Telephone Number and Organization.
   [redacted], **Deputy Director, Division of Risk, Strategy, and Financial Innovation,** [redacted]

2. Project Manager Name, Title, Telephone Number and Organization.
   [redacted], **Sr. Information Technology Specialist,** [redacted], **Office of Application and Software Development**

GENERAL INFORMATION - Project/System Information

1. Name of Project or System.
   Tips, Complaints, and Referrals (TCR) Intake and Resolution System

2. Description of Project or System.
   The TCR Intake and Resolution system will collect, store, review, circulate and analyze tips, complaints, and referrals received by the SEC from individuals concerning alleged violations of the federal securities laws. This system will implement flexible workflow, content management, and status tracking capabilities to support resolution processes as well as robust search and reporting for the management of TCRs.

3. What is the purpose of the Project or System?
   Provide a system for the SEC to manage tips, complaints, and referrals that are provided to the agency from investors, SEC staff and SEC partners, or anyone from the general public concerning alleged violations of the federal securities laws.

4. Requested Operational Date?
   December 2010

5. System of Records Notice (SORN) number?
   SEC-29, Agency Correspondence Tracking System; SEC-42, Enforcement Files; and SEC-55, Information Pertaining or Relevant to SEC Registrants and Their Activities currently cover TCR records for various offices and divisions. A comprehensive TCR SORN is currently in development to cover the agency-wide use of these records.

6. Is this an Exhibit 300 project or system?
   Yes

7. What specific legal authorities, arrangements, and/or agreements require the collection of this information?
   15 U.S.C. 77s, 77t, 78u, 77uuu, 80a-41, and 80b-9. 17 CFR 202.5

SECTION I - Data in the System

1. What data is to be collected?

The system will collect information about the individual making the complaint and/or information about the firm or individual the complaint is against including name, address, phone number, and e-mail address; and details about the complaint which may be provided in structured fields, free text, and related documents.

2. Is the Social Security Number (SSN) collected? (This includes truncated SSNs)
   The system doesn't ask for SSN; however, since many of the fields are free-form, if someone filing a complaint provides an SSN, it would be stored.

3. What are the sources of the data?
   Sources of the data include SEC personnel, investors and the general public, as well as broker-dealers, investment advisers, self-regulatory organizations (SROs), other government agencies, and foreign regulators.

4. Why is the data being collected?
   To allow the Commission the ability to identify and address securities fraud and misconduct more efficiently by implementing a comprehensive process for receiving, recording, tracking, and taking action on TCRs.

5. What technologies will be used to collect the data?
   A web-based application is used to collect data from external users and transmitted via a secure connection to the SEC server. External users will complete a web-based intake form to submit their information. Information received through other means, i.e. e-mails, phone calls, regular mail and personal interactions by staff, will be entered by SEC staff into the TCR system.

6. Does a personal identifier retrieve the data?
   A personal identifier is not required for data retrieval; however personal identifiers could be used to do so. Offices and divisions using the system may retrieve data via personal identifiers.

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

1. Describe the uses of the data.
   Data is used by SEC staff to determine if the alleged securities fraud or misconduct has occurred. Data is also used for purposes of measurement and monitoring, quality assurance, and research and analysis.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern?
   Yes. The system will have reports that can assist SEC staff in identifying areas of concern and patterns.

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   All information that is provided is maintained in the original state. SEC staff will review each complaint and perform regular analysis and testing on the accuracy of the data. Quality Assurance and Process Measurement, Monitoring, and Control methodologies have been developed and are being refined to validate the effectiveness of the SEC reviews.

SECTION III - Sharing Practices

1. Will the data be shared with any internal or external organizations?
   Data will be shared with other federal, state, local, or foreign law enforcement agencies; securities self-regulatory organizations; and foreign financial regulatory authorities for purposes of investigating, prosecuting, enforcing, or implementing the federal securities laws, rules, or regulations. Additionally, data may be shared with other organizations in accordance with the routine uses set forth in the Commission's System of Records Notice, SEC-42, Enforcement Files.

2. How is the data transmitted or disclosed to the internal or external organization or systems?
   The system will use Hypertext Transfer Protocol Secure (HTTPS) for the transfer of electronic data to other systems. **Transfer of data by other means such as paper, e-mails etc will be transferred in accordance with established SEC polices and procedures including SECR 24-04-A.01, "Rules of the Road."**

3. How is the shared data secured by external recipients?
   External Organizations are responsible for having in place a combination of physical security measures, policies/procedures, staff training, identification/authentication, and access controls to secure data.

4. Does the system receive or share Personally Identifiable Information (PII) with any other SEC systems, including systems hosted by an SEC contractor? If **YES**, list system name(s)
   - **Investor Response Information System (IRIS)**
   - **HUB SYSTEM**
   - **Risk Assessment Documentation and Inspection Umbrella System (RADIUS)**
   - **Active Directory (AD)**

SECTION IV - Notice to Individuals to Decline/Consent Use

1. Was notice provided to the different individuals prior to collection of data?
   Yes. Notice of this collection will be provided by a Privacy Act Statement on forms collecting information from the submitter, applicable SEC SORNs published in the *Federal Register,* and this PIA.

2. Do individuals have the opportunity and/or right to decline to provide data?
   Yes.

3. Do individuals have the right to consent to particular uses of the data?
   No. Individuals voluntarily provide the data collected and the individual is provided notice of the routine uses for that data via the applicable SORN, this PIA, and a Privacy Act Statement at the point of collection; however, the individual does not have the ability to limit or specify for which uses the data may be provided.

SECTION V - Access to Data (administrative and technological controls)

1. Has the retention schedule been established by the Records Officer?
   - If **YES**, what is the retention period for the data in the system?

   No. However, until such time as a retention schedule has been established by the Records Officer, 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 and as approved by the National Archives and Records Administration.

2. What are the procedures for identification and disposition of the data at the end of the retention period?
   The data will be identified and disposed of using the procedures stated above.

3. 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. Additional policies and procedures are being developed that will specify the requirements on protecting the data appropriately.

4. Will SEC contractors have access to the system?
   User access will be determined by the business owners on a case by case basis, and anyone with access must comply with the established policies and procedures.

5. Is the data secured in accordance with FISMA requirements?
   - If **YES,** provide date that the Certification & Accreditation was completed.

   The system is currently undergoing the C&A process.

6. Is the system exposed to the Internet without going through VPN?
   - If **YES**, is secure authentication required and is the session encrypted?

   The intake application completed by external users will be available without going through the VPN. The intake application has SSL.

7. Are there regular (i.e. periodic, recurring, etc.) data extractions from the system? If **YES,** describe the location of the extraction.
   Authorized SEC staff may extract data from the System in the form of reports and data files. Currently the authorized staff who will be performing these extracts reside at the SEC Headquarters Office in Washington, DC.

8. Which user group(s) will have access to the system?
   External users will have limited access for purposes submitting tips, complaints, and referrals via the web-based intake application. Only authorized staff of the Division of Enforcement, Office of Compliance Inspections and Examinations, Office of Investor Education and Advocacy, Division of Trading and Markets, Division of Investment Management, Division of Corporation Finance, Division of Risk, Strategy, and Financial Innovation, Office of International Affairs, Office of the Secretary, Office of Information Technology and Regional Offices will have access to the internal system.

9. How is access to the data by a user determined? Are procedures documented?
   Procedures are currently being developed that will describe how access to the data by a user is determined.
10. How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The system has user access controls in place to prevent non-privileged accounts from modifying system level files and accessing system data and resources without a valid need to know. The system owner will approve and designate the types of roles for personnel thru an approval process.

11. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
    Users will have specific levels of access privilege that will deny access to (or not display) information for which they are not authorized to browse, and each user will be trained to prevent misuse of data.

SECTION VI - Privacy Analysis

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

Most of the data is entered via a web application by the general public and other external entities in structured and unstructured fields. Files can also be attached to the tip, complaint, or referral. Since not all the data is structured, and individuals have the ability to attach files, the privacy risks are not fully known. There is nothing in the system to strictly prevent a member of the public to include PII in either an unstructured field or within an attachment. However, required security controls will be put into place to protect all of the data in the system. Also, C&A will be conducted to ensure the proper security controls have been put into place. In addition, the Division of Risk, Strategy, and Financial Innovation will conduct regular quality assurance and process monitoring activities to ensure proper security controls are in place.

Signature of Individual(s) completing this form

_____ _____

System Owner/Date Project Manager/Date

Endorsement

_____ _____

Chief Privacy Officer/Date Chief Information Security Officer/Date

Approval

_____

Chief Information Officer/Date