

U.S. Securities and Exchange Commission

**Tips, Complaints, and Referrals (TCR) Repository
PRIVACY IMPACT ASSESSMENT (PIA)**



September 30, 2013

Privacy Impact Assessment
Tips, Complaints, and Referrals (TCR) Repository

General Information

1. Name of Project or System.
Tips, Complaints, and Referrals (TCR) Repository
2. Describe the project and its purpose or function in the SEC's IT environment.
The TCR Repository is a read-only database of stored TCR's received by the SEC. The TCR Repository is capable of storing a wide range of artifacts such as documents, images, video and audio that are received with TCRs. Authenticated users have the ability to search and read the TCR Repository database for older TCR's submitted to the SEC prior to March 13, 2011.
3. Requested Operational Date? TCR Repository has been operational since November 2009. The most recent recertification for the system occurred on February 4, 2010. This PIA is being conducted to assess the current privacy risks and vulnerabilities of the data contained in the database. It should be noted that there is no longer any active data collection function being conducted in the TCR Repository database. Existing data in the TCR Repository is accessible in a read-only format.
4. System of Records Notice (SORN) number? SEC- 42, Enforcement 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. 77s, 77t, 78u, 77uuu, 80a-41, and 80b-9. 17 CFR 202.5.

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
Since March 13, 2011, there has been no active data collection in the TCR Repository. Previously, the system collected information about the individual making the complaint and/or information about the firm or individual the complaint is made against. This information can include submitter's and subject's 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. 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.
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?

Privacy Impact Assessment
Tips, Complaints, and Referrals (TCR) Repository

TCRs can come to the SEC through the web-based TCR External application, telephone calls, emails, and faxes or be received internally at the SEC via the TCR Internal application.

4. Why is the data being collected?
This information may be used to alert the SEC to misconduct or any unfair practice in the securities industry that may require regulatory review and/or investigation.
5. What technologies will be used to collect the data?
A web-based application was used to collect data from external users and transmitted via a secure connection to the SEC server. External users 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.

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 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? No Yes If yes, please explain: The system will have reports that can assist users 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.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
 No Yes If yes, please list organization(s): Data will be shared with other SEC offices and divisions for purposes of investigating, prosecuting, enforcing, or implementing the federal securities laws, rules, or regulations.
2. Will the data be shared with any external organizations?
 No Yes If yes, please list organizations(s): 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.

How is the data transmitted or disclosed to external organization(s)? 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

Privacy Impact Assessment
Tips, Complaints, and Referrals (TCR) Repository

accordance with established SEC policies and procedures including SECR 24-04-A.01, "Rules of the Road."

3. How is the shared data secured by external recipients?
ZixMail Email Encryption tool (SMAIL)
4. Does the project/system process or access PII in any other SEC system?
 No
 Yes. If yes, list system(s). Investor Response Information System (IRIS); Active Directory (AD)

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: All information is provided on a voluntarily basis. If desired, individuals can provide information anonymously.
3. Do individuals have the right to consent to particular uses of the data?
 Yes No N/A
Please explain: The SEC determines how provided data will be used in accordance with established policies and procedures.

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: Development of a records retention schedule is currently in progress.
 Yes If yes, list retention period:
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: 2/4/10
 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

Privacy Impact Assessment

Tips, Complaints, and Referrals (TCR) Repository

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?
Internal SEC Divisions and Offices (Enforcement, OCIE, DERA, IM, TM, Corp Fin, OGC, OCOO, Office of the Chairman, OCA, OIA, OIEA, OCR, All Regional Offices)
7. How is access to the data by a user determined? User access requests are submitted and approved by division/office designated TCR Point of Contact (POC). Once approved by POC, final approval is provided by DERA system administrators.
Are procedures documented? Yes No
8. How are the actual assignments of roles and rules verified?
All data in the TCR Repository is accessible as read-only data.
9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data? All users of the TCR Repository are limited to read-only access. Approval for system access is multi-tiered and closely monitored. User training is also provided to prevent misuse of system 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.

As previously mentioned, since March 13, 2011, the TCR Repository system has not actively collected data. All previously collected data in the system is accessible on a read-only basis. Most of the data previously collected in the system was entered via a web application by the general public and other organizations external to the SEC in structured and unstructured data entry fields. Submitter's can also attach files to the TCR form. Since not all of the data is structured, and individuals have the capability to attach files to the complaint form, the privacy risk are not fully known. There are no inhibitors in the TCR Repository to prevent the general public from including PII information in either an unstructured field or in an attachment to the complaint form. However, security controls are in place to protect data that has been collected in the system, and a C&A has been conducted to ensure proper security controls have been put in place. DERA does an annual review of users and removes access to users that no longer need access if that would help.