U.S. Securities and Exchange Commission

The Tips Complaints and Referrals (TCR) Modernization Project
PRIVACY IMPACT ASSESSMENT (PIA)

June 18, 2015

Office of Information Technology

Privacy Impact Assessment

Tips Complaints and Referrals (TCR) Modernization

General Information

1. Name of Project or System.
   The Tips Complaints and Referrals (TCR) Modernization Project.

2. Describe the project and its purpose or function in the SEC's IT environment.
   The Tips Complaints and Referrals (TCR) System is an agency-wide system that centralizes all Tips, Complaints or Referrals received by the SEC alleging possible violations of the federal securities laws and regulations thereunder. The mission of the U.S. Securities and Exchange Commission (the SEC or Commission) is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. In the pursuit of its mission, the SEC receives hundreds of thousands of incoming communications through a variety of means into each of the SEC's divisions, offices, and regions. These communications include tips and complaints from the general public, attorneys and members of the regulated community, which includes, but is not limited to, broker-dealers, investment advisors, and public companies. In addition, the SEC receives referrals from self-regulatory organizations (SROs) based on the information collected by the SROs and reported to the SEC for further consideration. The SEC's Office of Compliance Inspections and Examinations (OCIE) - in the course of conducting its examinations - creates referrals for the SEC's Division of Enforcement (Enforcement) to conduct further analysis and if warranted, undertake an investigation into possible allegations of violations of the federal securities laws and regulations. SEC divisions, offices, and regions also receive referrals from U.S. and foreign government agencies.

   The current TCR System will be modernized. The modernization will include both the External TCR Intake and Internal Components. The fundamental objective of the initiative is to modernize and implement an enterprise-class TCR System that is robust, flexible, and scalable, and can support the SEC's needs, mission and policies as they evolve over time. An important requirement of this project is to implement a more capable and user-friendly TCR System that possesses increased flexibility, configurability, and adaptability, and that more effectively supports TCR work processes. Additionally, the modernized TCR System must provide flexible and robust intake, triage, resolution, searching, and reporting functionalities with full auditing capabilities. The scope of this project includes conducting a detailed analysis, undertaking architecture and design, and executing implementation and delivery of a modernized TCR System. High-Level Core Capabilities will include: implementing a new Intake Form, a more efficient reassignment and workflow process, a Whistleblower Information Tracking Module and Context Based Help and a robust search capability.

3. Requested Operational Date? Aug 05, 2015

4. System of Records Notice (SORN) number?
   SEC-63 "Tips, Complaints, and Referrals" and 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. 77a et seq., 15 U.S.C. 78a et seq., 15 U.S.C. 80a-1 et seq., 15 U.S.C. 80b-1 et seq., and 5 U.S.C. 302. Also SEC Rules 21F-1 through 21F-17 under 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?
   Name, date of birth, social security number, mailing address, email address, telephone number, tip, complaint and referral information including allegation descriptions dates, and supporting details, supporting documentation, web forms, emails, criminal history, financial holdings and account information, working papers of the staff and other documents and records relating to the matter.

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 TCR System does not request SSNs, but individuals may choose to provide their SSN during the process of submitting TCR. In some cases, the SEC may request an SSN to resolve a TCR when the submitter uses that number as a way to identify an account. The legal authority for collecting SSNs is Executive Order 9397, as amended by Executive Order 13478.

3. What are the sources of the data?
   Tips, complaints, and referrals can come to the SEC through the web-based TCR External application, telephone calls, emails, facsimiles, and internally via the TCR Internal application.

4. Why is the data being collected?
   The data is collected to alert the SEC to possible violations of the federal securities laws that may require regulatory review and/or investigation.

5. What technologies will be used to collect the data?
   Databases, Middleware, and HTTP/HTTPS servers.

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 violations of the federal securities laws occurred. Data is also used for purposes of measurement, monitoring, quality assurance, and research 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 uses technology to conduct electronic searches, queries, or analyses, and to generate reports that can assist users in identifying areas of concern and/or patterns.

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   External intakes and internal intakes will collect data from individuals. The accuracy of the intakes will be determined via follow-up during the TCR triage and disposition process.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   □ No ☒ Yes If yes, please list organization(s):
   Authorized staff throughout the SEC will have access to the data in the modernized TCR system.

2. Will the data be shared with any external organizations?
   □ No ☒ Yes If yes, please list organizations(s):
   Data will be shared with certain other U.S. regulators, 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.

   How is the data transmitted or disclosed to external organization(s)?
   Data is shared with external organizations via secure encrypted email. Transfer of data will be in accordance with established SEC policies and procedures for electronic transmission of personally identifiable information and sensitive data.

3. How is the shared data secured by external recipients?
   Data is shared using encryption technology . Recipients secure the data in accordance with applicable government and/or industry policies and procedures for sensitive personal information, including secure system accesses. Shared data may also be secured in accordance with SEC or other nondisclosure agreements or MOUs or court protective orders.

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

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 voluntary 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: By voluntarily submitting a TCR, an individual effectively consents to all uses of the information outlined in the Privacy Act Statement, SORN, and other privacy notices provided.

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: A proposed record retention schedule for TCR records is pending with NARA, and generally provides for a 20 year retention schedule for TCR System records. The SEC will maintain TCR records indefinitely until NARA approves a record retention schedule. Records that fall under a general record retention schedule will be disposed of according to the applicable schedule.
   □ Yes If yes, list retention period:

2. What are the procedures for identification and disposition of the data at the end of the retention period?
   The precise procedures for identification of the data at the end of the retention period are still under discussion and to be determined, but are likely to rely on date stamps, system logs, case status data, and/or other relevant information captured by the TCR system. Disposition of the data will be in accordance with the SEC's NARA-approved record retention schedules and applicable SEC administrative regulations and Records Management Directives.

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. Staff also take periodic training on records management and the protection of SEC non-public information.

   A TCR User Guide will be provided to the user community. The TCR team will also conduct Instructor Led Training (ILT), Computer Based Training (CBT), and other supplemental materials to assist users.

4. Has a system security plan been completed for the information system(s) supporting the project?
   ☒ Yes If yes, please provide date SA&A was completed: June 2014
   □ No If the project does not trigger the SA&A requirement, state that along with an explanation

5. 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

6. Are there regular (i.e. periodic, recurring, etc.) PII data extractions from the system?
   ☒ No ☐ Yes If yes, please explain:

7. Which user group(s) will have access to the system?
   All SEC Offices and Divisions except the Office of Financial Management (OFM), Office of Information Technology (OIT), Office of Human Resources (OHR), and Office of Support services (OSO). The Office of Information Technology (OIT) access is primarily for system administration purposes.

8. How is access to the data by a user determined?
   a. Authentication - Internal users must be valid SEC users, with valid Active Directory/Windows accounts, and permission via supervisor notice and approval to the TCR system in order to gain access. Additionally, the Oracle Identity Management System Security module enforces SEC security standards for locking users due to repeated, failed access attempts or password expiration.

   b. Authorization – The TCR Modernization system contains extremely complex business rules in support of user permissions within the application, to limit access to a need-to-know for supporting valid business purposes.

   Are procedures documented? ☒ Yes ☐ No
   The TCR User Guide identifies permissions for approximately 30 TCR features/functions across a variety of user roles.

9. How are the actual assignments of roles and rules verified?
   The Division of Economic and Risk Analysis (DERA) has an auditable process in place to assign users to relevant groups and roles based on their need-to-know, and rules of the system.

10. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
    SEC has implemented a rigorous set of security controls for the TCR system, and has limited access to those SEC employees who have a clearly defined business need to know the information. Regular periodic checks within DERA will occur to monitor user access. Additionally, certain roles and rights will be established in the system to prevent unauthorized users from accessing areas and data within the application for which they are not approved. System audit and logging functionality can identify and deter unauthorized use of the system.

SECTION VI - Privacy Analysis

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

– There is a risk that individuals who submit a TCR could provide more information than is necessary to resolve or respond to the TCR. To help mitigate that risk, the TCR Portal is a web form that directs individuals to submit only that information which is necessary to resolve or refer their TCR. The SEC provides security and privacy training to its employees who collect TCR via the telephone calls, emails and faxes.

- A privacy statement on the intake form, and user access to other applicable privacy notices (SORN, Privacy Impact Assessment, web privacy policy) outlines the reasons for the collection of information, and how the information is used.

- There is also a risk that individuals could unnecessarily provide their SSN. Though the SEC does not request SSNs, individuals may choose to provide their SSN during the process of submitting TCR, and in some cases, the SEC may request an SSN to resolve a TCR when the submitter uses that number as a way to identify an account. The SEC has built-in processes and controls to limit the chance of a SSN being included when it is not necessary. Trained employees guide individuals who choose to submit TCRs via telephone on what information to provide when making a complaint.

- The SEC does not validate the information at the time it is initially collected, but may validate at a very basic level in the course of referring or responding to a TCR. Therefore, there is a risk associated with data quality and integrity. To help mitigate that risk, the SEC follows up when something is incorrectly noted.

- Because the TCR System includes large amounts of information related to possible violations of the federal securities laws and regulations, it may be considered a rich target for hackers, identity thieves, and other cyber-threats. The SEC has mitigated this risk by implementing extensive security controls and safeguards for the TCR System to protect information contained in the system against unauthorized disclosure and access.

- The SEC only grants access to the system to authorized users who, based on their need to know, are restricted to the minimal amount of data required or appropriate to carry out their assigned job responsibilities. Access is terminated or reduced as necessary should the employee or contractor no longer have a need to know the information, change job functions, be terminated, or resign.

There is a risk that TCRs could be filed on behalf of individuals without their consent. To mitigate this risk, the SEC's complaint intake form requires individuals filing TCRs on behalf of other individuals to identify at least one point of contact (telephone number or email or physical address) for the submitter and/or attorney for a whistleblower submission.