U.S. Securities and Exchange Commission

Tips, Complaints and Referrals Intake and Resolution (TCR) 3.0
PRIVACY IMPACT ASSESSMENT (PIA)

April 23, 2020

Division of Enforcement

Section 1: System Overview

1.1 Name of Project or System

Tips, Complaints and Referrals Intake and Resolution (TCR) 3.0

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) SEC Wide

☐ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed: 3/1/2011

Last updated: 6/18/2015

Description of update: The TCR System -- both External TCR Intake and Internal components -- has been redesigned and updated. The redesigned system (TCR 3.0) provides an updated and user-friendly complaint entry form. It contains new user functionality and features relating to TCR business and workflow processes, and provides enhanced tracking and auditing capabilities. It also features enhanced TCR search capabilities and functions, including a keyword search feature and ability to search TCR attachments.

1.4 Does the system or program employ any of the following technologies?

☐ Enterprise Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☐ Cloud Computing Services

☒ www.sec.gov Web Portal

☐ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

The mission of the Securities and Exchange Commission ("SEC") is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. In pursuit of its mission, the SEC utilizes the Tips Complaints and Referrals 3.0 ("TCR") system to intake and process tips and complaints alleging possible violations of Federal securities laws. Submission may be received from the general public (whistleblowers and non-whistleblowers), attorneys, broker-dealers, investment advisors, public companies and other members of the regulated community, and referrals from Self-Regulatory organizations (SROs) and U.S. and foreign government agencies and store them in a centralized database. The Division of Enforcement's Office of Market Intelligence ("OMI") is the business owner of TCR, but several divisions and offices agency-wide use the system.

TCR consists of a web application with two interfaces; (1) an external, public-facing web complaint form (Accessible by public with no authentication needed), and (2) an internal system (accessible by authorized SEC employees and contractors only). The external component is the TCR web complaint form. The public can access the web form by clicking the "Submit a Tip or File a Complaint" button on the SEC main website at https//www.sec.gov/tcr. The internal system is used by SEC staff to review, process, and assign TCRs within the agency and to document staff research, findings, and actions or decisions taken on TCRs. The internal system is also used by SEC staff to search TCRs. When submitting a TCR, the complainant must include the name of at least one subject of the complaint (e.g., an individual, entity, social media account name, or website) and a description of the alleged wrongdoing. The complainant is also required to indicate whether he or she is filing the tip under the SEC's Whistleblower Program and, in some instances, to provide the name and contact information for any attorney representing them in connection with their whistleblower complaint.

Non-whistleblowers who submit TCRs and whistleblowers represented by counsel may choose to submit their TCR anonymously. TCR submitters may choose, but are not required to, submit their own contact information or contact information of the subject(s) they are complaining about (e.g., addresses, telephone numbers, email addresses, etc.).

TCR submitters can choose to upload and submit supporting documents or other materials with their TCR form. Once an individual completes and submits the TCR form, the information is saved in a database and the system returns a unique submission number confirming the submission. Designated SEC staff then review, research, and evaluate the TCR, document their findings and recommendations, and either close the TCR with a recommendation for no further action by the SEC, or assign the TCR onward to staff in the appropriate offices/divisions to consider for potential further investigation, examination, or other response or closure with no further action.

A new user must obtain approval from their office/division TCR Point of Contact (POC) to access the TCR 3.0 Internal system. The POC submits an access request to the TCR Business Support team ("TCR Support"). TCR support will then review the request and, if granted, assign the user the appropriate role and corresponding privileges in the system. Only certain, authorized users are granted the roles and privileges that enable them to take certain actions or view certain information in the system. For example, only certain assigned roles allow internal users to assign and take action on

TCRs, create or edit TCR records or add attachments, upload comments and notes in the system, disposition (close) TCRs, view secured information, and/or update whistleblower related information. All internal user roles, however, have the ability to search and view TCR records.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

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.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No

☐ Yes

If yes, provide the purpose of collection:

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No

☐ Yes, a System of Record Notice (SORN) is in progress

☒ Yes, there is an existing SORN

SEC-63 "Tips, Complaints, and Referrals" and SEC-42 "Enforcement Files."

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☐ No

☒ Yes

Electronic Data Collection System-Tips, Complaints, Referrals (TCR) OMB Number: 3235-0672 (exp. 2/28/2022)

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The purpose of the collection is to intake and process tips, complaints, and referrals alleging possible violations of Federal securities laws. The privacy risk identified is the over-collection of information and potential disclosure of sensitive personally identifiable information (PII). There is also a risk that information collected as part of a complaint or comment may be used inappropriately or may be used for purposes beyond the purpose or intent of the information collection.

To mitigate these risks, the TCR complaint form only requests information that is necessary for the purpose of the information collection and limits the amount of information that is mandatory or required for submission to subject name, description of complaint (alleged wrongdoing), and statutorily-required information relating to whistleblower status. Information that is required and that

which is optional is clearly identified on the form. The form also provides submitters the option to submit complaints anonymously.

The privacy risks are also mitigated by system access controls and auditing capabilities. System users are assigned specific roles that provide system access and privileges as needed to perform specific job duties, or to provide support for development and Operation and Maintenance (O&M) functions of the system. Additionally, all system users are subject to TCR-specific and general SEC policies regarding access and use of information and are required to complete training regarding the handling and use of information, including privacy and information security awareness training. Finally, the privacy risks are mitigated by deployment of encryption of data in accordance with NIST standards.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☐ Social Security Number	☐ Alien Registration	☐ Financial Accounts
☐ Taxpayer ID	☐ Driver's License Number	☐ Financial Transactions
☐ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☐ File/Case ID	☐ Credit Card Number	☐ Employer ID

☒ Other: Although the system does not require any of the information listed in order to file a complaint, the individual submitting the web form may choose to provide any of the information listed. In addition, the SEC personnel reviewing and researching the complaint as part of the triage process, may enter any of the above information in a text field or upload a document/enter a note containing the above information.

General Personal Data

☒ Name	☐ Date of Birth	☐ Marriage Records
☒ Maiden Name	☐ Place of Birth	☒ Financial Information
☒ Alias	☒ Home Address	☐ Medical Information
☐ Gender	☒ Telephone Number	☐ Military Service
☐ Age	☒ Email Address	☐ Mother's Maiden Name
☐ Race/Ethnicity	☐ Education Records	☐ Health Plan Numbers
☐ Civil or Criminal History	☒ Zip Code	

☒ Other: Although the system does not require any of the information listed in order to file a complaint, the individual submitting the web form may choose to provide any of the information listed. In addition, the SEC personnel reviewing and researching the complaint as part of the triage process, may enter any of the above information in a text field or upload a document/enter a note containing the above information.

Work-Related Data

☒ Occupation	☒ Telephone Number	☐ Salary
☒ Job Title	☒ Email Address	☐ Work History
☒ Work Address	☐ Certificate/License Number	☐ Business Associates
☐ PIV Card Information	☒ Fax Number	

☒ Other: Although the system does not require any of the information listed in order to file a complaint, the individual submitting the web form may choose to provide any of the information listed. In addition, the SEC personnel reviewing and researching the complaint as part of the triage process, may enter any of the above information in a text field or upload a document/enter a note containing the above information.

Distinguishing Features/Biometrics

☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature
☐ Other:		

System Administration/Audit Data

☒ User ID	☒ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☒ Queries Ran	☐ Contents of Files
☐ Other:		

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

Data including PII is used to intake complaints that alert the SEC to possible violations of securities laws, to evaluate and process complaints, and to investigate, prosecute, examine or inspect, or take other action in response to the complaints. Data is also used for purposes of measurement, monitoring, quality assurance, and research analysis. Information provided for the SEC's whistleblower award program pursuant to Section 21F of the Securities Exchange Act of 1934 (Exchange Act) may be used in connection with an evaluation of a whistleblower's eligibility and other factors relevant to the Commission's determination of whether to pay an award. Information may also be used in connection with system audits, to track and enable auditing of workflow, assignments, and actions taken on TCRs.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees

Purpose: Information collected from SEC employees such as SEC User ID and date/time of access occurs as part of their duties to enter, triage and resolve TCRs and support their office/division mission and information technology systems. The information collected from SEC employees relates to the underlying work and system administration, controls, and audits.

☒ SEC Federal Contractors

Purpose: Information collected from Federal contractors such as SEC User ID and date/time of access occurs as part of their duties to enter, triage and resolve TCRs and support their office/division mission and information technology systems. The information collected from Federal contractors relates to the underlying work and system administration, controls, and audits.

☒ Interns

Purpose: Information collected from Interns such as SEC User ID and date/time of access occurs as part of their duties to support their office/division mission. The

information collected from interns relates to the underlying work and system administration, controls, and audits.

☒ Members of the Public

Purpose: Information is collected on complaint submitters and on subjects of complaints to alert the SEC to possible violations of the Federal securities laws and to evaluate the complaint and investigate, prosecute, examine or inspect, or take other action in response to the alleged wrongdoing. Data is also used for purposes of measurement, monitoring, quality assurance, and research analysis.

☐ Employee Family Members
Purpose:

☐ Former Employees
Purpose:

☐ Job Applicants
Purpose:

☐ Vendors
Purpose:

☐ Other:
Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

An Authorization to Test (ATT) was approved in order to conduct User Acceptance Testing in the Production (PROD) environment with actual TCR data before the system going live. The Stage environment was deemed not suitable for adequate or accurate testing at the time the risk acceptance was granted. As a condition to granting the ATT, SEC data was removed from all environments when no longer needed. Training efforts that may involve access or use of actual TCR records, which may contain PII, are limited to users who have been authorized and granted access to view this information.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☐ No.

☒ Yes. DAA-0266-2018-0009

3.6 What are the procedures for identification and disposition at the end of the retention period?

There are capabilities that enable the system to create records based on fielded data such as date of TCR submission and date of TCR disposition. The system administrators have the capability to delete records that meet the retention criteria. There are reporting tools that are able to generate a report identifying all of the TCRs meeting the destruction policy criteria in the calendar year. The procedures for identification rely on considerations such as date stamps, system logs, case status data,

and/or other relevant information captured by the TCR system. Disposition of the data is in accordance with the SEC's NARA-approved record retention schedules and applicable SEC administrative regulations and Records Management Directives.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A

☐ Members of the Public
Purpose:

☐ Employees
Purpose:

☐ Contractors
Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

There is a privacy risk that individuals who submit a TCR could voluntarily provide more information than is necessary to resolve or respond to the TCR, including PII. To mitigate this risk, the TCR complaint form only requests information that is necessary for the purpose of the information collection and limits the amount of information that is mandatory or required for submission to subject name, description of complaint (alleged wrongdoing), and statutorily-required information relating to whistleblower status. Information that is required and that which is optional is clearly identified on the form. The form also provides submitters the option to submit complaints anonymously. Additionally, the SEC has the ability to secure notes or documents in the event that there is sensitive information so that only those users with secure access may view the information. The SEC has published SORN SEC-63 in the Federal Register and on its own website to serve as public notice to individuals that certain PII, including SSN, could be contained in the TCR system. As a safeguard, data collected and stored in the TCR System is encrypted in accordance with National Institute of Standards and Technology (NIST) standards.

There is a privacy risk that information collected as part of a complaint or comment may be for purposes beyond the purpose or intent of the information collection. To mitigate this risk, the system has access controls and auditing capabilities to ensure authorized users are accessing information in an appropriate manner. All system users are also subject to SEC policies regarding access and use of information and are required to complete training regarding the handling and use of information, including privacy and information security awareness.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☒ Privacy Act Statement
The Privacy Act Statement is available to users after accepting the TCR portal web disclaimer.

☒ System of Records Notice

SEC-63 "Tips, Complaints, and Referrals" and SEC-42 "Enforcement Files."

☒ Privacy Impact Assessment
Date of Last Update: 6/18/2015

☒ Web Privacy Policy
The Web Privacy Policy is accessible via https://www.sec.gov/privacy.htm.

☒ Other notice:
Filing Guidance and Confidentiality. https://www.sec.gov/complaint/info

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

Insufficient notice of the routine uses of the data collected is an identified privacy risk. This risk is mitigated by the published SORNs, SEC-63 and this privacy impact assessment (PIA). Both documents are published on the SEC's website to provide notice of how the SEC uses the information collected by the system. A Privacy Act Statement is posted on the external TCR Complaint Form web portal. For information collected through official forms (Form TCR) and entered into the system by SEC staff, notice may be provided at the original point of collection on the forms.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

After a TCR is submitted into the TCR System, it is reviewed and assessed by designated SEC staff who have been assigned specific roles and privileges in the system that allow them to access a TCR inbox within the system. The TCR System also provides authorized users with the ability to query and search the system for TCR records by keyword or certain data fields. Certain business intelligence, analytics, and reporting tools may be used by authorized users to access or ingest TCR data. The TCR data may be used to generate reports, dashboards, or other business intelligence or analytical products for operational purposes, to determine whether any person has violated, is violating, or is about to violate provision of the federal securities laws or rules, or to investigate possible violations of the federal securities law.

5.2 Will internal organizations have access to the data?

☐ No

☒ Yes

Organizations: The majority of SEC Offices and Divisions have users that can search and view TCR submissions and associated data relating to workflow and assignments; research, findings and recommendations; and disposition.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

Information may be inadvertently disclosed or shared with unauthorized individuals. These risks are mitigated by implementing role-based access controls. Access permissions for System Administrators are restricted to the organizations for which they are responsible. All system users are subject to policies regarding access and use of information and are required to complete training regarding the handling and use of information, including privacy and information security awareness.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: The TCR System does not provide direct access to external organizations for information sharing. The SEC may disclose the information within TCR pursuant to the routine uses identified in SEC's Tips, Complaints, and Referrals and Enforcement Files Systems of Records, and as otherwise authorized under the Privacy Act. The information collected and retained in the TCR system may be shared under certain circumstances to coordinate law enforcement activities between the SEC and other federal, state, local or foreign law enforcement agencies, securities self-regulatory organizations, and foreign securities authorities; and pursuant to other routine uses as described in SEC-42 "Enforcement Files." Certain information may be redacted from the data, if required, before it is shared.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

There is a risk of unauthorized disclosure to a third party. This risk is mitigated by transmitting the data through secure channels, such as encrypted email, with appropriate data sharing agreements in place to ensure parties understand the safeguards for handling the information. Sensitive PII may also be redacted before information is shared.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☒ Directly from the individual.
☒ Other source(s): Attorneys and agents acting on behalf of an individual or entity can submit TCRs. Internal SEC users can submit TCRs based on information received from external sources. Self-regulatory organizations, exchanges, and other foreign and domestic government agencies and third parties can submit referrals as well.

6.2 What methods will be used to collect the data?

Data is collected through the web-based TCR External application. Internal SEC users can submit TCRs based on information received from external sources through telephone calls, emails, facsimiles, and mail via the TCR Internal application. Additionally, some data entered

into the SEC's IRIS system is submitted into the TCR system.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

The data collected from individuals through the web-based TCR External application contains data input validations to ensure data consistency (e.g., zip codes are numeric, there is a zip code autosuggest, logic for a point of contact, phone numbers are numeric). Individuals completing the web form receive a summary of the information they provided and can review and edit their answers to the form questions before they electronically submit the form to the SEC. After individuals complete and submit the web form, they receive an automated response confirming that their submission has been received successfully by the system. This confirmation page also generates and displays a unique submission number for the TCR and displays all information entered by the individual in response to the form questions. Individuals are able to print and save a copy of this confirmation page, which lists their TCR submission number and data submitted. Certain authorized users can perform manual updates to TCR records if requested. Individuals may also submit additional or updated information related to their TCR through the TCR system to change or update information that is erroneous, inaccurate, or irrelevant.

6.4 Does the project or system process, or access, PII in any other SEC system?

☐ No
☒ Yes.
System(s): The SEC's IRIS system has a submission of TCR data that contains PII

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

There is a privacy risk that TCR may contain inaccurate or outdated information. This risk is mitigated by collecting information directly from the source via the public-facing web portal. Additional information can be submitted to correct any inaccuracies, and certain authorized users can perform manual updates or corrections to records if requested. Additionally, there is a risk of over-collection of information, which may impact data integrity. To mitigate this risk, the TCR complaint form only requests information that is necessary for the purpose of the information collection and limits the amount of information that is mandatory or required for submission to subject name, description of complaint (alleged wrongdoing), and statutorily-required information relating to whistleblower status.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Individuals agree to voluntarily submit a TCR and provide the information in support of their TCR. Individual use of the system to provide information is strictly voluntary. Individuals may choose to submit the complaint anonymously in which case the first and last name fields are populated automatically with the word "ANONYMOUS" and the home telephone field is

populated with zeros. The amount of information that is mandatory or required for submission of a TCR is limited.

7.2 What procedures are in place to allow individuals to access their information?

Individuals seeking notification of and access to any record contained in this system of records may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549-2736.

After individuals complete and submit their answers to the web form, they receive an automated response confirming that their submission has been received successfully by the system. This confirmation page also generates and displays a unique submission number for the TCR and displays all information entered by the individual in response to the form questions. Individuals are able to print and save a copy of this confirmation page, which lists their TCR submission number and data submitted.

7.3 Can individuals amend information about themselves in the system? If so, how?

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549-2736.

7.4 Discuss the privacy risks related to individual participation and redress. How were these risks mitigated?

The primary risks are lack of access to information and inability to seek redress and correction. This risk is mitigated by providing individual access or correction of the records as expressly permitted by the Privacy Act and provided by the FOIA. If individuals are not satisfied with their ability to update their information within TCR submitted by third parties, they may file a Privacy Act Request. In addition, individuals may submit additional or updated information related to their TCR through the TCR system to change or update information that is erroneous, inaccurate, or irrelevant.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes

8.2 Can the system be accessed outside of a connected SEC network?

☐ No

☒ Yes (NOTE: the above is for the External TCR system.)

If yes, is secured authentication required?	☒	No	☐	Yes	☐	Not Applicable
Is the session encrypted?	☐	No	☒	Yes	☐	Not Applicable

8.3 Does the site have a posted privacy notice?

☐ No
☒ Yes
☐ N/A

8.4 Does the project or system use web measurement and/or customization technologies?

☒ No
☐ Yes, but they do not collect PII

☐ Yes, and they collect PII

8.5 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

The primary privacy risk is inadvertent or unauthorized disclosure of information to individuals. This risk is mitigated by implementing role based access controls and privileges, general access, and password control. Access permissions to System Administrators are restricted to the organizations for which they are responsible. Records are encrypted and maintained in a secured environment with access limited to authorized personnel whose duties require access. User accounts are synched with SEC's Active Directory.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC users complete the Privacy and Information Security Awareness training prior to being granted access to SEC information and information systems. In addition, users are trained on SEC Rules of the Road governing their activities related to safeguarding SEC information. Privacy and Information Security Awareness is provided on a continuous basis to keep users alert to the privacy and security requirements and safeguards.

9.2 Does the system generate reports that contain information on individuals?

☐ No
☒ Yes

Reporting tools can be used with the system to generate reports containing TCR data. Reports using TCR data may be shared internally/externally via secure encrypted email. Transfer of data is in accordance with established SEC policies and procedures for electronic transmission of

personally identifiable information and sensitive data. Sensitive PII data may be redacted prior to sharing with outside organizations.

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, MOUs, or court protective orders.

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☐ No
☐ Yes
☒ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes

The system and the platform on which the system resides provide logging and auditing capabilities. Assignments, actions taken on TCRs, and updates or changes to the TCR record are logged by the system. TCR records are auditable by when an action was performed on the record (e.g., field updates, uploading of documents, assignment of TCRs, addition of notes and comments), by when the action occurred, and by the user who took the action. The system's platform also employs audit or event logging relating to user access including dates and time of access, session duration, and search terms queried. Audit record content includes: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Although access to this system is limited only to authorized SEC staff, the expected residual risk related to access, given the sensitivity of the PII in the system, can include the inadvertent handling or misuse of data. Examples include but are not limited to the unauthorized distribution of PII, sharing of username and password credentials, and sharing proprietary system information. To mitigate this risk, user accounts for employees are synched with SEC's Active Directory and system privileges are granted based on defined roles.