U.S. Securities and Exchange Commission

Enforcement Applications Platform (EAP)
PRIVACY IMPACT ASSESSMENT (PIA)

August 29, 2025

Division of Enforcement

/Publication History

Revision	Date	Changes Made
Initial	01/01/2007	Original Document
1	08/29/2025	Review and Update

Privacy Impact Assessment

Enforcement Applications Platform (EAP)

Section 1: System Overview

1.1 Name of Project or System

Enforcement Applications Platform (EAP)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) — If the system is internally hosted, please list the Division or Office.

☒ 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: 1/1/2007

Last updated: 8/14/2025

Description of update: OWB Release 27.2: NoCA Exports, Draft links, Higher visibility of Promote from Hub, More info in Claimant's Claim grid, Adjust document types, Legal Summary layout changes, Task tag visibility changes, Bug fixes

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

☒ Enterprise Data Platform (EDP)

☐ Social Media

☒ Mobile Application (or GPS)

☒ Cloud Computing Services

☒ www.sec.gov Web Portal

☒ Artificial Intelligence (AI)

☐ 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

EAP houses four modules used by the Division of Enforcement (ENF). All modules have internal and external hosting:

- The HUB) module used by ENF to manage cases. The system uses roles to assign privileges to users of the system based on the role of the user. Upon the completion of a satisfactory request for access, the following groups in ENF, and internal to the Securities and Exchange Commission (SEC) will have access to HUB: ENF attorneys, accountants, paralegals, legal technicians, case management specialists, certain approved contractors and other ENF staff working on or supporting those who are working on investigations and litigation.
- The Whistleblower module is used to manage and support the Office of the Whistleblower (OWB) by tracking cases, payments, collections, payment approvals, workflows, Congressional inquiries and Office of the Inspector General (OIG) and Freedom of Information Act (FOIA) requests.
- The Tax and Fund Administrator Management System (TFAMS) module enables ENF staff to store communications with and documentation received from fund and tax administrators, track and sort information by case names and numbers and assign/review workloads and provide reporting capabilities to serve the Office of Distribution's analytical needs.

- The Tips, Complaints and Referrals (TCR) System module is an agency-wide system that centralizes all TCRs received by the SEC alleging possible violations of the Federal Securities laws.
    - The mission of the SEC is to protect investors, maintain fair, orderly, and efficient markets; and facilitate capital formation. In the pursuit of its mission, the SEC receives thousands of incoming communications. 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. Self-regulatory organizations (SROs) make referrals to the SEC. Numerous SEC divisions and offices may enter TCRs for consideration by other SEC divisions and offices. For example, the Division of Examinations (EXAMS), while conducting its examinations, creates referrals for ENF to conduct further analysis and undertake an investigation into possible allegations of violations of Federal Securities laws. The SEC also receives referrals from U.S. and foreign government agencies.
    - The current TCR system, both external TCR intake and internal components, has been redesigned. The external component is accessed by the general public via SEC's external-facing web site (www.sec.gov). Once taken to an acceptance disclaimer page (and accepting), the user is then directed to the welcome page for TCR. Here they can find pertinent information about instructions for submitting a complaint form, uploading documents, and information on the SEC's Whistleblower program. They can file a Tip, Complaint, or Referral as well as submit supporting documents. Once the form is completed and submitted by the public, the form data and documents are saved in the TCR repository (on Amazon Simple Storage Service), called TCR intake. The external users are then provided a unique submission number confirming the submission. The submitted form data shows up in the inboxes of the SEC Internal users with privileges to see this data. Internal SEC users then make updates to the data, upload/create notes and documents, and send the TCRs through the business triage process where proper actions are taken by the appropriate users. The TCR system employs the use of Artificial Intelligence (AI) for identifying submissions related to cryptocurrency assets and generation of submission summaries.

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

Securities Exchange Act of 1933, Sections 15 U.S.C. 77s, 77t, and 77uuu; Securities Exchange Act of 1934, Section 78u; Investment Company Act of 1940, Section 80a-41; and Investment Advisors Act of 1940, Section 80b-9; 17 CFR 202.5

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:	The Commission may use SSNs to identify individuals for ENF purposes. The TCR system does not request SSNs in any complaint form, question or instructions, but submitters may provide their SSNs or those of subjects during the process of submitting TCRs – in the form or in an attachment.
If yes, provide the legal authority:	Executive Order 9397

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

☐ No
☐ Yes, a SORN is in progress

☒ Yes, there is an existing SORN
SEC-17 Enforcement Files, 85 FR 85440, January 27, 2021
SEC-29 Tips, Complaints and Referrals Records, 85 FR 85440, January 27, 2021

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

☒ No
☐ Yes
If yes, please cite all relevant OMB collection numbers and their expiration dates.

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

The primary privacy risk for this data collection is unauthorized or inadvertent disclosure of sensitive personally identifiable information (SPII) or non-public investigatory material or case information. This risk is mitigated by implementing strict role-based access controls (RBAC); requiring Commission staff and supporting contractors to submit access requests to the System Owner, which are granted on a valid need-to-know/need-to-share basis and determined by assigned official duties.

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: Whistleblower ID

General Personal Data

☒ Name	☐ Date of Birth	☐ Marriage Records
☒ Maiden Name	☐ Place of Birth	☒ Financial Information
☒ Alias	☒ Home Address	☐ Medical Information
☒ Sex	☒ 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 TCR system does not require any SPII to file a complaint, individuals submitting the TCR web form may enter any of 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 TCR system does not require any SPII to file a complaint, individuals submitting the TCR web form may enter any of the above information.

Distinguishing Features/Biometrics

☐ Fingerprints	☐ Photographs	☐ Genetic Information
☒ Voice Recording	☐ Video Recordings	☐ Voice Signature

☐ Other: Click here to enter text.

System Administration/Audit Data

☒ User ID	☒ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☒ Queries Ran	☐ Contents of Files
☐ Other: Click here to enter text.		

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

The HUB system collects data from direct entry by the ENF Staff. The HUB system tracks Matters Under Investigation (MUIs), Investigations, Actions, related party information, and other ENF-related data. ENF staff uses the data collected for the management of the cases and the reporting of Division case-related metrics.

A TCR is any credible allegation or statement of concern about a possible violation of the federal securities laws or conduct that poses a possible risk of harm to investors. PII is collected to alert the SEC to possible violations of the federal securities laws that may require regulatory review and/or investigation.

No PII is collected or stored by the TFAMS module. OWB does not collect or use SSN. OWB collects Name, Phone, Address, and Email as part of the workflow for cases.

The system requires that the individual submitting the tip or complaint provide the name, address, and contact information of the alleged wrongdoers. The submitter may provide name, address, and contact information that will be entered by SEC into TCR. Although contact information will aid the SEC in investigating and prosecuting alleged violations of the federal securities laws that have occurred, individuals may choose to submit the complaint anonymously. Data is used by SEC staff to investigate the alleged violations of the federal securities laws.

Data is also used for purposes of measurement, monitoring, quality assurance, and research analysis.

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

☒ SEC Employees
Purpose: Track staffing information and usage of employees in the system.

☒ SEC Federal Contractors
Purpose: Track staffing information and usage of contractors in the system.

☒ Interns
Purpose: Information collected from Interns occurs as part of their duties to support their office/division mission. The information collected from interns relates to the underlying work and could include their SEC UserID.

☒ Members of the Public
Purpose: The information collected is to support ENF Matters Under Inquiry (MUI), Investigations, and/or Actions. The HUB module of EAP collects data from direct entry by ENF Staff. The HUB system tracks MUIs, Investigations, Actions, related party information, and other ENF-related data. ENF staff uses the data collected for the management of the cases and reporting of Division case-related metrics.

☐ Employee Family Members
Purpose: Describe the purpose of collecting the information from this source.

☒ Former Employees
Purpose: Track staffing information and prior usage by employees in the system.

☐ Job Applicants
Purpose: Describe the purpose of collecting the information from this source.

☐ Vendors
Purpose: Describe the purpose of collecting the information from this source.

☐ Other: List other sources of information.
Purpose: Describe the purpose of collecting the information from this source.

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

Authorization to Test (ATT)-00039 was issued to authorize the use of production data for testing in the EAP stage environment. For minimization efforts, information is redacted by ENF staff within the production EAP system without use of any other tools. For example, redaction may be performed to protect the identity of whistleblowers. In most situations, PII is not altered in order to preserve authenticity of documents. Additionally, redaction may be performed to limit access to privileged information (which may or may not include PII). Additionally, the system collects required PII through use of a data entry form which is designed as a web form so that individuals submit only that information which is necessary.
For any additional testing, training and/or research efforts conducted in lower environments, an ATT will be obtained.

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

☐ No.
If no, provide an explanation for the absence of a NARA schedule.
☒ Yes.
Division of Enforcement Case Management and Tracking System HUB schedule: DAA-0266-2019-0001-0001.
Whistleblower Application Files OWB schedule: DAA-0266-2019-0003-0001.

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

The HUB system retention schedule identifies the cut off at the end of the calendar year when case is closed or becomes inactive. The proposed schedule for HUB system data is that data will be destroyed/deleted 50 years after cutoff or when no longer needed for business purposes. The schedule has been approved by NARA. Additionally, the OWB system's retention schedule cuts off after the whistleblower's appeals of decisions are exhausted or after the last award payment to the whistleblower is made, whichever is applicable, and whichever is later. Data will be destroyed/deleted 10 years after the cutoff.

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

☒ N/A
☐ Members of the Public
Purpose: If the system or project monitors the members of the public, explain the purpose of the monitoring.
☐ Employees
Purpose: If the system or project monitors employees, explain the purpose of the monitoring.
☐ Contractors
Purpose: If the system or project monitors contractors, explain the purpose of the monitoring.

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 provide more information than is necessary to resolve or respond to the TCR. To mitigate this risk, the TCR Portal is designed as a web form so that individuals submit only that information, which is necessary to resolve or refer their TCR, and none of the required fields are SPII. Also, the SEC provides information security and privacy training to its employees who may come in contact with a tip via phone calls, mail, emails and faxes.

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
SEC Form 1661: "Privacy Act of 1974" noted on page 4 under Section G.13 Routine Uses of Information
SEC Form 1662: "Privacy Act of 1974" noted on page 4 under Section H.13 Routine Uses of Information
When an individual/member of the public clicks on the TCR URL on www.sec.gov it is displayed

☒ System of Records Notice
SEC-17 Enforcement Files, 85 FR 85440, January 27, 2021
SEC-29 Tips, Complaints and Referrals Records, 85 FR 85440, January 27, 2021

☒ Privacy Impact Assessment
Date of Last Update: 3/7/2025

☒ Web Privacy Policy
https://www.sec.gov/welcome-tips-complaints-and-referrals

☒ Other notice:
https://www.sec.gov/enforcement-litigation/whistleblower-program

☐ Notice was not provided.
If no notice was provided, please explain why not.

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

There is a risk that individuals included in investigative materials are not made aware of the collection of their information. This privacy risk is inherent given the nature of investigative process and the material gathered, and often the individuals whose information may be found in the documents are sometimes not the suppliers of the information. However, the SEC has taken steps to mitigate this risk by providing transparency through the publication of this PIA and SORNs SEC-17 and SEC-29. Also, the law enforcement exemption is applicable insofar as investigatory materials are compiled for law enforcement purposes are collected.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

The HUB module of EAP does not analyze data to derive new data or create previously unavailable data about an individual through aggregation from the information collected.

The OWB module of EAP does not analyze data to drive new data or create previously unavailable data about an individual. OWB approves whistle blower case payment(s) and track those payment(s).

TCR data is used by SEC staff to determine if the alleged violation(s) of Federal securities laws occurred.

TCR Redesign Data is also used for purposes of measurement, monitoring, quality assurance, and research analysis. The data is used to conduct searches, DB queries, analyses, and to generate reports that can assist users in identifying areas of concern and/or patterns. In addition, where feasible, SEC staff manually validates the data and corrects input errors. The staff then performs triage and disposition of TCRs.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: The following user groups in ENF, and those internal to the SEC, have access to the HUB system: ENF staff working on, or supporting those working on, investigations and litigation generally has access to the HUB system, upon completion of a satisfactory request for access. This includes ENF attorneys, accountants, paralegals, legal techs, Case Management Specialists, and certain approved contractors. The system uses roles to assign privileges to users of the system based on the role of the user.

Outside of the ENF, a limited number of accounts are provided to staff from other SEC Divisions and Offices through a robust approval process which is managed by ENF Corporate Finance (CF), Division of Economic Risk Assessment (DERA), Investment Management (IM), Trading and Markets (TM), Office of Chief Operating Officer (OCOO), Division of Examinations (EXAMS), Office of Credit Ratings (OCR), Office of the Ethics Council (OEC), Office of Financial Management (OFM), Office of the General Council (OGC), Office of Human Resources (OHR), OIG, Office of International Affairs (OIA), Office of Investor Education and Advocacy (OIEA), Office of Public Affairs (OPA), Office of the Secretary (OS) to provide ENF information for use in the pursuit of their objectives.

The HUB system also has interconnections with other SEC systems that are governed by ASIs (Agreement to Share Information). These agreements detail what data is transferred from the HUB system and at what frequency.

TCR data is available to the majority of SEC Offices and Divisions.

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

A privacy risk associated with internal sharing is that SPII in the HUB system could be erroneously or inadvertently disclosed. This privacy risk is mitigated by implementing RBACs; limiting sharing of SPII with downstream applications; and executing Agreements to Share Information (ASIs) with any SEC Division or Office that has a system with which the ENF shares information. The ASIs are system specific, (e.g. Enterprise Business Intelligence Reporting (EBIR) [MicroStrategy]) and are signed by both parties and renewed periodically detailing what fields are shared. They include the recipient's need for HUB system data, the number of users, data to be provided, system security requirements, and other terms.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: TCR data will be shared with certain other U.S. regulators, other federal, state, local, or foreign law enforcement agencies, securities SROs, and foreign financial regulatory authorities for purposes of investigating, prosecuting, enforcing or implementing the federal securities laws, rules or regulations.

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

HUB system data is not shared with external entities.
Only TCR data has the potential to be shared with external organizations via secure file transfer and/or encrypted email. Transfer of data will be in accordance with established SEC policies and procedures for electronic transmission of PII and sensitive data. Staff are trained on redaction of SPII data prior to sharing with outside organizations. Data is shared using encryption technology. Recipients have the responsibility to secure the data in accordance with applicable government and/or industry policies and procedures for sensitive personal information, including secure system accesses. Shared data must also be secured in accordance with SEC or other nondisclosure agreements or MOUs or court protective orders.

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): ENF staff and users have access to the HUB system and have privileges to add content. ENF may receive information from many sources during an investigation. ENF may receive documents from other government, administrative or law enforcement agencies. In an investigation, multiple requests for information could also result in information being provided by several branches of a corporate entity, in addition to individuals. Depending on the circumstances, documents may be provided directly by an individual or by the individual's corporate employer. Attorneys and agents acting on behalf of an individual or entity can submit TCR. Internal SEC users, outside entities - foreign and domestic, submit referrals as well.

6.2 What methods will be used to collect the data?

ENF staff manually upload documents to the HUB system. The data comes from various sources including internal documents, action memos and Federal Court records. Staff can search a Master Entity list to add entities one at a time to a matter.

TCRs can come to the SEC through the web-based TCR External application, telephone calls, emails, facsimiles, hard copies and internally via the TCR Internal application.

Delphi Transaction File (DTF) payments data is ingested into the OWB module. OWB approves the payment for whistle blower cases after they have been adjudicated. DTF is the payment tracking system. OWB ingests DTF data to verify payment and track balances.

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

Data quality is governed by internal guidance for accuracy which involves referencing supporting documentation. The HUB system is supported by documentation to perform cross-checks to ensure data quality and integrity.

TCR has fields in the complaint form that have validation logic to ensure data consistency. The main check on this data is done during triage by trained SEC personnel. To ensure data quality and accuracy, SEC personnel will research materials; conduct the proper due diligence before taking adverse action against an individual; maintain chain of custody records for the documents to demonstrate how they were received and processed; and verify through testimony and litigation the accuracy of the documents and data.

OWB uses the same table and database as Hub. Hub and OWB may have different views, but the database is the same. Data accuracy is verified by cross reference with other SEC systems.

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

☐ No
☒ Yes.
System(s): Enterprise Human Capital Repository System (EHCR) – Retrieves SEC Employee and Contractor information. The Investor Response Information System (IRIS) has a submission of TCR data that can contain 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?

The primary privacy risk is that the Commission may rely on outdated or inaccurate information. Where feasible, data collected in the HUB, OWB, and TFAMS modules is supported by documentation, thus minimizing risks to data quality and integrity.

The SEC does not validate the information at the time it is initially collected, but may validate at a very basic level, while referring or responding to a TCR. Therefore, there is a risk associated with data quality and integrity. The quality and the integrity of the data a primarily dependent on the submitter. To mitigate this risk, SEC does not make any changes to the data from the original submission but can add to the data during the triage process.

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.

Where information is sought from individuals, disclosures are made in such forms as SEC Forms 1661 and 1662. Individuals from whom information is sought voluntarily have the right to decline to provide it.

Individuals from whom information is sought via subpoena may decline to provide information pursuant to a subpoena based upon a valid assertion of privilege, Fifth Amendment, or other legitimate basis. Such assertions may be litigated depending on the facts and circumstances of the assertion.

Individuals do not have the right to consent to uses of the data for the same reasons stated above.

By voluntarily submitting a TCR, an individual effectively consents to all uses of the information outlined in the Privacy Act Statement and SORNs SEC-17 and SEC-29, this PIA and other privacy notices. The SORNs and this PIA are available on the public facing web site, www.SEC.gov. Additionally, individuals may choose to submit a TCR anonymously.

OWB collects Name, Phone, Address, and Email as part of the workflow for cases and ingests DTF data to verify payment and track balances.

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

The SEC gives individuals the ability to request access and amendment to their personal information in accordance with the Privacy Act and the SEC's Privacy Act regulations at 17 CFR Part 200 Subpart H. Although individuals may request access to information about themselves contained in an SEC system of record through the SEC Privacy Act/FOIA procedures, ENF records are exempt from the access and correction provisions of the Privacy Act (see SORN SEC-17). This system is exempted from the Privacy Act insofar as it contains law enforcement investigatory materials.

Individuals can access and review their data prior to submission of the TCR. Once submitted, they would need to contact the SEC to make any requests for additions or corrections.

Because HUB, OWB & TFAMS data are not submitted by individuals of the general public, this section would not apply to those modules, only TCR, which is submitted by individuals.

Individuals may submit a request by directly contacting the SEC's FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or submit a request electronically to foiapa@sec.gov or online.

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

As mentioned above, individuals may request access to and correction of their information under the SEC Privacy Act/FOIA procedures, however, the data may be exempt from access and correction provisions under the Privacy Act and therefore access to such records will be restricted. Individuals may submit a request by directly contacting the SEC's FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or submit a request electronically to foiapa@sec.gov or online.

Once an individual submits TCR data, they cannot alter their submission, but they can contact SEC and submit a correction.

HUB, OWB, and TFAMS data is not submitted by individuals of the general public. This section would not apply to those modules, only TCR, which is submitted by individuals.

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

Given that individuals are not generally permitted to access or correct records about themselves available in the HUB system, there is a risk that inaccurate or erroneous information about an individual could be used by SEC personnel. This system is exempted from the Privacy Act insofar as it contains investigatory materials. This system is exempted from the Privacy Act insofar as it contains investigatory materials compiled for law enforcement purposes. This risk is mitigated by SEC personnel researching materials; conducting the proper due diligence before taking adverse action against an individual; maintaining chain of custody records for the documents to demonstrate how they were received and processed; and verifying through testimony and litigation the accuracy of the documents and data.

As mentioned above, individual accepts the risks by voluntarily submitting the information. 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. To mitigate this risk, individuals may choose to submit a TCR anonymously.

Section 8: Security

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

☒ No (HUB, OWB, TFAMS)

☒ Yes (TCR)

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

8.2 Does the project or system involve an online collection of personal data?

☐ No

☒ Yes

Public URL: https://www.sec.gov/files/formtcr.pdf

8.3 Does the site have a posted privacy notice?

☐ No
☒ Yes
☐ N/A

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 staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII. SEC Technology Rules of Behavior ensure that employees and contractors are aware of their security responsibilities and how to fulfill them.
In addition, the HUB/OWB/TFAMS/TCR User Guides available either during onboarding or in the respective module of the EAP.

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

☐ No
☒ Yes

Application reports are only available to those that have access to the relevant module of EAP. Reports differ by module. Reports can be downloaded from the application, and the standard SEC rules governing protection of PII would apply. Users can only download reports containing data which they are permitted to see.

Reports are kept internal to the SEC and shared via SharePoint, where permissions are configured for least privilege. Under rare circumstances, reports may need to be shared with other Federal authorities.

Additional reports (e.g. management reports) can be generated and are summary in nature and do not generally contain PII and outside the application. However, these reports are treated with the same confidentiality as application reports.

Reports using TCR data may be shared with internally/externally via secure encrypted email. Transfer of data will be in accordance with established SEC policies and procedures for electronic transmission of PII and sensitive data. Staff are trained on redaction of SPII data 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 or 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 EAP system offers monitoring of security events through its auditing reporting feature and allows audit tables and reports that system administrators can use to monitor login, searches, views, and saves. The system also logs security-related events, including changes to reference data, recording who made the change and when. The system also logs who views audit reports and when; this will allow system owners to increase the granularity and frequency of audits in response to a perceived change in the threat environment.

The Audit record content for the EAP includes, for most audit records: (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.

The TCR System captures: Business Process Management (BPM)workflow and logs the following events: 1) Start of task 2) Completion of task 3) Update of a task (including reassignments) The following information is captured: 1) Date-Time of the action 2) Action name 3) Submitted by user 4) Submitted by user's group 5) Associated workflow comments 6) Received user 7) Received user's group.

Authorization: 1) Users with the role "TCR_ADMIN" should be able to view these audit records on the front end and users with TCRINTKAE DB privileges (read/write) should be able to read them from database.

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.

Residual risk to privacy is limited, however system administrators can increase the permissions for roles, modify security parameters, and logging settings in order to keep the risk to privacy minimal. These actions will be logged.