U.S. Securities and Exchange Commission

Case Tracking and Records Retention System (CTaRRS)
PRIVACY IMPACT ASSESSMENT (PIA)

July 20, 2017

Office of the General Counsel

Privacy Impact Assessment

Case Tracking and Records Retention System (CTaRRS)

Section I: System Overview

1.1 Name of Project or System

Case Tracking and Records Retention System (CTaRRS)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC)

☐ 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:

Last updated:

Description of update:

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

☐ Electronic 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

CTaRRS is a case tracking system designed to electronically manage each Office of General Counsel (OGC) case through its lifecycle in a centralized location. The system will serve primarily as a case tracking system, but will also include document repository and records management functionality for files and records related to cases in the system. CTaRRS will directly support core OGC functions related to providing legal guidance and representation to the Commission and constituent offices, and will facilitate information reporting by OGC management on cases.

The system will contain information related to individual cases and matters handled by OGC staff, such as factual background about the matter, staff notes, matter status, legal research, legal memoranda, case filings, calendar and schedule information, and emails. Typical transactions performed by the system include saving case/matter data input by SEC users; searching case/matter data; generating reports on case/matter data; and providing user alerts and notices. The system will permit sharing of case/matter information with other authorized users who have system permissions that warrant access to the particular information.

The system is a browser-based web application that requires several plug-ins or add-ons to facilitate compatibility with Microsoft Office and Adobe. The collected information related to individual cases and matters handled by OGC staff will reside on in a Microsoft SQL database maintained by the SEC.

Users will need to establish user accounts to access or view information in the system. User accounts require a valid license seat, to be purchased by the SEC. The SEC will have access to user account information. Users will

access the system from their SEC-issued computers or using authorized SEC remote access technology using the browser-based application.

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

15 U.S.C. § 77s, 77sss, 78d(b), 78w, 80a-37, 80b-11.

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

☐ No
☒ Yes

If yes, provide the purpose of collection: Social Security numbers may be contained in personnel files relevant to employment cases handled by OGC. Social security numbers of persons related to investigations may be contained in files relevant to the Division of Enforcement (ENF) matters on which OGC provides support, and in Appellate and Adjudication case files.

If yes, provide the legal authority: Executive Order 13478; Sections 19(c) and 20(a) of the Securities Act of 1933; Section 21(a) of the Securities Exchange Act of 1934; Section 321(a) of the Trust Indenture Act of 1939; Section 42(b) of the Investment Company Act of 1940; Section 209(b) of the Investment Advisors Act of 1940; and 17 C.F.R. §§ 200.21, 201.102(e), 202.5(a).

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-31, Office of the General Counsel Working Files

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

☒ No
☐ Yes

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

The primary privacy risks are that personal information may be collected without a clear purpose or without clear legal authority; information collected is either unnecessary or excessive; or the information provided for one purpose may be used inappropriately. These potential risks are mitigated by clearly stating the purpose for collecting the personal information in the applicable systems of records notices, privacy impact assessments and other notices, and limiting the information collected to what is truly necessary for intended purposes.

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:		

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:		
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:		
Distinguishing Features/Biometrics		
☐ Fingerprints	☒ Photographs	☐ Genetic Information
☐ Voice Recording/Signature	☒ Video Recordings	
☐ Other:		
System Administration/Audit Data		
☒ User ID	☒ Date/Time of Access	☒ ID Files Accessed
☒ IP Address	☒ Queries Run	☒ 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?

PII is collected, used, shared or maintained as a part of various underlying OGC case files that are contained in CTaRRS. For instance, Financial Account and Financial Transaction information may constitute relevant factual information in Adjudication and Appeals case files and in General Litigation matters supporting ENF cases. Work-Related Data and General Personal Data may constitute relevant factual information in 102(e) and employment case files. And System Administration/Audit Data will be maintained by CTaRRS to validate system security and authorized use policies. All data is used to facilitate handling and management of OGC matters.

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

☒ SEC Employees
Purpose: May be factually relevant in employment and related cases handled by OGC.

☒ SEC Federal Contractors
Purpose: May be factually relevant in contracts and related cases handled by OGC.

☒ Interns
Purpose: May be factually relevant in employment and related cases handled by OGC.

☒ Members of the Public
Purpose: May be factually relevant in 102(e), adjudication, appellate, and in general litigation matters supporting ENF cases.

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: May be factually relevant in employment and related cases handled by OGC.

☒ Job Applicants
Purpose: May be factually relevant in employment and related cases handled by OGC.

☒ Vendors
Purpose: May be factually relevant in contracts and related matters handled by OGC.

☐ Other:
Purpose:

3.4 What mechanisms are in place to minimize the use of PII for testing, training, and research efforts?

PII is not used for testing, training, and/or research efforts. The system collects the minimally required PII to manage each OGC case through its lifecycle.

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

☒ Yes.
Records in CTaRRS are governed by existing records schedules approved by NARA. The records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with record schedules of the SEC.

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

Records that have reached the end of their retention period will be identified by notices, alerts, and/or searches within CTaRRS. Disposition of records will be facilitated by CTaRRS, which contains a requirement for the ability to export records and metadata in a format acceptable for transfer to NARA. The procedures for identification and disposition are maintained in applicable guidance on an OGC SharePoint site for OGC Records Management.

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

☐ N/A

☐ Members of the Public
Purpose:

☒ Employees
Purpose: The system contains audit capabilities that track user access to and actions within CTaRRS. To the extent this functionality constitutes monitoring, the purpose is to ensure the system is accessed and used only by authorized users to further official SEC business.

☒ Contractors
Purpose: The system contains audit capabilities that track user access to and actions within CTaRRS. Some CTaRRS users may be contractors supporting OGC activities. To the extent this functionality constitutes monitoring, the purpose is to ensure the system is accessed and used only by authorized users to further official SEC business.

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

The primary privacy risk is inadvertent or unauthorized access/disclosure of nonpublic information. This risk is mitigated by ensuring that CTaRRS utilizes granular access controls (by group, user type, case type, and/or record type) to protect the data at all levels and deployment of encryption of data-at-rest in accordance with NIST standards and role-based access. Additionally, the system will employ audit capabilities to ensure system access and use is appropriate. The system will leverage Active Directory for authentication to further mitigate the potential for unauthorized access of data. All users are required to take mandatory training on Cyber Security

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

☒ System of Records Notice
SEC-31 and SEC-42 (for ENF support matters).

☒ Privacy Impact Assessment
Date of Last Update: Current PIA

☐ Web Privacy Policy

☒ Other notice:
SEC Forms 1661 or 1662 are also provided for certain OGC-initiated collections made by subpoena or discovery. For OGC matters in support of ENF cases, ENF may have provided notice by SEC Forms 1661 or 1662 at initial information collection.

☐ Notice was not provided.

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

Given that the purpose of CTaRRS is to maintain case file information input by SEC users, and the information is covered by multiple SORNs and other notices, the primary risk is inadequate notice. Individuals may not be aware that information is being collected, who will use it or the purpose for which information may be used; information may be out of date or irrelevant for intended purpose; or individuals maynot be able to update their information if they do not know OGC has it. This potential risk is mitigated by ensuring that SORNs are current and adequately cover all CTaRRS information and PIA reports are published and adequately describe how personal information will be managed.

Section 5: Limits on Uses and Sharing of Information

5.1 What types of methods are used to analyze the data?

Data is analyzed via search and reporting capabilities, which may present existing information in the form of graphs, charts, and related management metrics. The system does not otherwise analyze or derive new information.

5.2 Will internal organizations have access to the data?

☒ Yes

Organizations: Authorized OGC staff will have access to the data. Data will be transmitted or disclosed via the internally-hosted CTaRRS application (Legal Files).

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

The primary privacy risks associated with internal sharing are inadvertent or unauthorized disclosure of nonpublic information to individuals without authorization; personal information collected may be used without legal authority by receiving office; or information is disclosed for a use not directly related to the primary purpose of the collection. These risks will be mitigated by ensuring that appropriate privacy protections are transferred along with the information through contractual arrangements, e.g., MOU; and removal of unnecessary identifying details before releasing the information.

5.4 Will external organizations have access to the data?

☒ No

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

Information will not be shared with external organizations.

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): All data is input by authorized SEC users. Depending on the type of OGC matter, information may be collected by staff directly from the individual or obtained from other sources. Other sources may include other Offices or Divisions of the Commission.

6.2 What methods will be used to collect the data?

All data will be entered into the system by OGC staff. Depending on the type of OGC matter, information may be collected by subpoena or discovery, voluntary submissions, or shared by other Offices or Divisions for OGC support or review.

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

The data in the system will be subject to standard supervisor oversight and peer review on a case-by-case basis. Information collected from individuals that is subject to an adversarial process also provides the individuals opportunities to address accuracy and completeness. System authentication and audit capabilities will ensure data integrity.

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

☒ No

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 risks are failing to limit edit-access to data or to limit, monitor and enforce access controls; and making decisions that impact negatively on individuals from incomplete or incorrect information. These potential risks are mitigated as the data in the system will be subject to standard supervisor oversight and peer review on a case-by-case basis. Also, in litigation and adversarial matters, there is ample opportunity for individuals to identify quality issues with factual information. In addition, system authentication and audit capabilities will ensure data integrity.

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 to be included in CTaRRS is sought voluntarily, individuals may decline to provide information. Where information is sought by subpoena, discovery, or other legal provision, individuals have the rights afforded by law. SORN SEC-31 and/or SEC-42, and SEC Forms 1661 and/or 1662, as applicable, may inform individuals about the collection and rights they may have to decline or opt out.

7.2 What procedures will allow individuals to access their information?

Persons wishing to obtain information on the procedures for gaining access to the contents of records may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736. See SORN SEC-31.

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

Persons wishing to obtain information on the procedures for amending information about themselves in the system may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736. See SORN SEC-31.

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

The primary privacy risks are lack of access to personal information and changes to systems of records that impact retrieval of information. These risks are mitigated by ensuring that SORNs are current and adequately cover procedures for participation and redress and PIA reports are published and adequately describe how personal information will be managed. Individuals will be notified of procedures for participation and redress via SORN SEC-31 and/or SEC Forms 1661/1662, and will have other applicable legal rights for information collected via discovery, subpoena, or related legal process.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ No
Project/application has not been scheduled for SA&A.

8.2 Identify individuals who will have access to the data in the project and state their respective roles.

☒ Users
Roles: Edit case data and reports

☒ Contractors
Roles: Edit case data

☒ Managers
Roles: Edit and review case data and reports

☐ Program Staff
Roles:

☐ Developers
Roles:

☒ System Administrators
Roles: Manage access/permissions, make configuration changes, and perform other administrative actions in support of the system.

☐ Others:
Roles:

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

☒ No

8.4 How will the system be secured?

Single Sign-on (SSO) authentication will be used. The system can be setup for PIV authentication as well.

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

☒ No

8.6 Does the site have a posted privacy notice?

☒ No.

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

☒ No

8.8 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 failing to limit edit-access to data, or to limit, monitor or enforce access controls, which can lead to misuse or unauthorized disclosure. This risk is mitigated by SSO. Users will access the system from their SEC-issued computers or using authorized SEC remote access technology using the browser-based application. Active Directory requires two-factor authentication and ensures the highest level of security.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system or project.

Users take regular mandatory training on Cyber Security and Privacy Awareness, Protecting Nonpublic Information, and Records Management. Additionally, CTaRRS-specific training will be provided to users.

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

☐ No

☒ Yes

The system has the capability to generate reports, and those reports could potentially contain information on individuals. Any reports will be handled in accordance with applicable records regulations and policies.

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

System audit capabilities will log system activities and data changes by user, and audit logs will be available to system administrators. Logs will be reviewed on an annual basis.

9.5 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?

The records are protected from unauthorized access through password and/or PIV card authentication (using Active Directory), role-based access, firewalls, and other system-based protections. System audit capabilities will log system activities and data changes by user, and audit logs will be available to system administrators.

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

Although the system will maintain sensitive PII, the manner of use and the system and user safeguards will largely mitigate the risks. Expected residual risk related to access is minimal.