U.S. Securities and Exchange Commission

Registrant Tracking System (RTS) Cloud
PRIVACY IMPACT ASSESSMENT (PIA)

February 19, 2025

Division of Examinations

Publication History

Revision	Date	Changes Made
Initial	5/25/2020	Original Document
1	9/4/2024	Review and Update
2	2/19/2025	Update for compliance with E.O. 14168

Section 1: System Overview

1.1 Name of Project or System

Registrant Tracking System (RTS) Cloud

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally Hosted (Contractor or other agency/organization) Amazon Web Services (AWS)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed:	5/25/2020
Last updated:	09/04/2024
Description of update:	To upgrade from RTS v1.14 to RTS v1.16

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

☐ 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

Registrant Tracking System (RTS) Cloud is an internally developed Division of Examinations (EXAMS) application hosted by Amazon Web Services. The system allows staff to enter, manage, and report on pre- and post-examination related communication, data, and documents from or about regulated entities and individuals. It also serves as the registration filing system for Bank Transfer Agent (TA) registrants.

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

15 U.S.C. 78a *et seq*., 80a-1 *et seq*., and 80b-1 *et seq*.

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:	Not Applicable
If yes, provide the legal authority:	Not Applicable

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-25 Information Pertaining or Relevant to SEC Regulated Entities and Their Activities, 85 FR 85440 (January 27, 2021).

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 principal privacy risk is the over collection of information of monitored entities and contacts. This risk is mitigated using data only from authorized external sources with specific legal authorities, arrangements, agreements and/or notice requirements that allow for information collection, as well as data provided by users modifying RTS information.

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

General Personal Data

☒ Name
☐ Maiden Name
☐ Alias
☐ Date of Birth
☐ Place of Birth
☐ Home Address
☐ Marriage Records
☐ Financial Information
☐ Medical Information

□ Sex
□ Age
□ Race/Ethnicity
□ Civil or Criminal History
□ Telephone Number
□ Email Address
□ Education Records
□ Zip Code
□ Military Service
□ Mother's Maiden Name
□ Health Plan Numbers
☒ Other: Central Registration Depository (CRD) Numbers, sanction information from Form U4.

Work-Related Data

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

Distinguishing Features/Biometrics

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

System Administration/Audit Data

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

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

EXAMS uses PII to monitor Entities and Contacts.

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

☒ SEC Employees
Purpose: The application audit logs record SEC Employees' activities in RTS.

☒ SEC Federal Contractors
Purpose: The application audit logs record SEC Federal Contractors' activities in RTS.

□ Interns
Purpose: Not Applicable

☒ Members of the Public
Purpose: Information from members of the public is used to monitor entities and contacts.

□ Employee Family Members
Purpose: Not Applicable

□ Former Employees
Purpose: Not Applicable

□ Job Applicants
Purpose: Not Applicable

□ Vendors
Purpose: Not Applicable

□ Other:
Purpose: Not Applicable

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

Corrections to the copy of work email, work phone, and work address stored in the Enterprise Data Warehouse (EDW) automatically flow to RTS. Where work email, work phone, or work address are explicitly flagged as personal information (e.g., a sole proprietor reports their own information as their "work" information), the system does not pull or store the data.

Non-production environments, used for testing and training, pull data solely from the corresponding non-production EDGAR and FINRA environments. Where live data is required for testing or training, the project team works with the Office of Information Technology (OIT) Security on an Authorization to Test (ATT) for a temporary duration. Any data used for a temporary duration would be deleted at the conclusion of the training.

Copies of work-related data elements in production may be part of research efforts staff complete to effectively monitor entities and contacts across their respective regions and registrant populations.

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

☐ No.

☒ Yes.
Disposition Authority Number DAA-0266-2013-0004-0002 - "Office and Compliance Inspections and Examinations Records"

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

A report is run to identify records held beyond the retention period of ten years. The System Administrator, or their designee, coordinates with the EXAMS Records Liaison to submit SEC Form 2889 to delete/destroy records beyond the retention period.

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

☐ N/A

☒ Members of the Public

Purpose: The application ingests and stores, among other things, associated persons names, addresses, telephone numbers, and email addresses from external sources as part of EXAMS' ongoing efforts to monitor contacts.

☐ Employees

Purpose:

☐ Contractors

Purpose:

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

Privacy risk associated with the type of information collected is unauthorized disclosure of information. This risk is mitigated by restricting system access to only authorized users and implementing role-based access control.

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
Not Applicable
☒ System of Records Notice
SEC-25 Information Pertaining or Relevant to SEC Regulated Entities and Their Activities. 85 FR 85440 (January 27, 2021).
☒ Privacy Impact Assessment
Date of Last Update:
☐ Web Privacy Policy
☒ Other notice:
Notice may be provided at the original point of collection. (e.g., Exam Staff present SEC Form 1662 and SEC Form 2866 to Registrants at the outset of an examination before data is finalized in TRENDS)
☐ 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?

There is no risk to privacy regarding notice because adequate notice is provided as identified in Section 4.1.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

RTS does not analyze data.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: Users from any SEC Division or Office can access data for review only in RTS if they are assigned a valid application role in the system. RTS also shares data with the EDW when it publishes a materialized view of bank-regulated transfer agent data.

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 the subsequent disclosure of the system information to unauthorized individuals within SEC divisions and offices. Limiting information or access to RTS Cloud to authorized personnel with official duties mitigates this risk.

5.4 Will external organizations have access to the data?

☒ No
☐ Yes

Organizations:

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

There is no risk to external sharing because information is not shared externally.

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): RTS ingests information from the SEC's Enterprise Data Warehouse (EDW).

6.2 What methods will be used to collect the data?

RTS ingests data from EDW using extract-transform-load (ETL) jobs in IBM DataStage. RTS does not collect information directly from individuals or companies. The individuals and companies in question submit registration data, and corrections thereto, to 1) the Commission's Electronic Data Gathering and Retrieval (EDGAR) system and 2) the Financial Industry Regulatory Authority, Inc. (FINRA). A copy of that registration data is stored in the Commission's Enterprise Data Warehouse (EDW) and RTS retrieves and stores a copy of a subset of that registration data from the EDW. Corrections automatically flow to RTS.

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

RTS does not perform data quality checks for accuracy and completeness but relies on the source system(s) where data is initially collected to check for data quality.

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

☐ No

☒ Yes.

System(s): RTS ingests PII from EDW.

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 related to data quality and integrity is that data in the system may be incomplete and/or inaccurate. This risk is minimized because information is checked for accuracy and completeness when it is collected by the source system. In additional the ETL process used to ingest data into RTS is reverified before any requested changes are deployed to production.

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 do not have the option to decline or opt of providing their information to RTS Cloud because information RTS does not collected information directly from individuals.

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

Individuals cannot directly access their information in RTS Cloud. However, they may submit a written request for access to FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549-2736 or may submit online at https://www.sec.gov/page/office-foia-services.

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

Individuals seeking access to their information in a source system that provides information to RTS Cloud, may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736, or email request to foiapa@sec.gov.

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

There is minimal to no privacy risk related to individual participation and redress because RTS is not the source system for collecting information from individuals.

Section 8: Security

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

☒ No
☐ Yes

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: None

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

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 initial and annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security responsibilities and how to fulfill them.

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

☐ No

☒ Yes

RTS connects with MicroStrategy for reporting purposes. The MicroStrategy reports that users can generate in RTS may contain regulated Entities' and their Associated Persons' names, addresses, telephone numbers, and email addresses. Additionally, there may be information relating to the business activities of regulated Entities and their Associated Persons, as well as their compliance with provisions of the federal securities laws and other applicable rules.

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

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.

Privacy risk related to access is minimal because information in transit and at rest is encrypted and secure user authentication, along with role-based access control, is performed as described in section 8.4.