U.S. Securities and Exchange Commission

eD2.0 Recommind
PRIVACY IMPACT ASSESSMENT (PIA)

August 8, 2019

Division of Enforcement

Privacy Impact Assessment

eD2.0 Recommind

Section 1: System Overview

1.1 Name of Project or System

eD2.0 Recommind

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Division of Enforcement

☐ 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: 4/24/2012

Last updated: 4/25/2012

Description of update: Updated for version 5 of software, no changes in the types of data collected, or how the data is used or shared.

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 main objective of the eD2.0 project is to replace the current version of Concordance. The eD2.0 Recommind Axcelerate is used by Enforcement Division to assist in managing their complex litigation needs. Because of its capabilities in managing case files, the system is also used at the SEC by the Office of Compliance Inspections and Examinations (OCIE), the Office of the General Counsel (OGC), the Office of Credit Ratings (OCR) and the Office of the Inspector General (OIG) by having separate instances of the same product. The eD2.0 application was implemented to reduce the complexity of the paperwork associated with the SEC's civil enforcement actions. It provides a platform to collect, manage, and maintain an extensive repository of electronic images relating to case files, primarily depositions, testimonies, proceedings, case notes, trial exhibits, and other enforcement and court related data. eD2.0 Recommind Axcelerate enables users to easily search and review thousands of documents effectively and efficiently. Users can quickly and easily organize their documents through the use of tags, annotation of transcripts, reports and complex search queries.

eD2.0 Recommind is a centrally managed data and document repository for documents received by the SEC in the course of examinations, investigations, and litigation. The SEC does not specifically request personally identifiable information (PII), but PII may be included in the documents the SEC receives. The documents are sometimes indexed and stored by a custodian's name. The eD2.0 Recommind data for a case can be searched

by PII values, such as a person's name or email address. Documents could include: investigative testimony, hardcopy evidence, forensics, audio evidence, financial statements, and court transcripts.

The purpose of upgrading the eD2.0 Recommind system to Axcelerate 5.x software is to take advantage of product enhancements. .

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

15 U.S.C. 77s, 77t, 78u, 77uuu, 80a-41, and 80b-9. 17 CFR 202.5

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

☒ No
eD2.0 Recommind does not collect SSNs. The Enforcement Division is not able to control what information is provided to the SEC by outside parties, so documents and data provided in response to subpoenas and voluntary document requests may contain SSNs or other PII. Thus, eD2.0 Recommind may maintain SSNs contained in third party productions given to the SEC. If provided, the legal authority to maintain the collection is 15 U.S.C. 77s, 77t, 78u, 77uuu, 80a-41, and 80b-9. 17 CFR 202.5.

☐ Yes
If yes, provide the purpose of collection:
If yes, provide the legal authority:

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-42, Enforcement Files. Depending on the type of documents received within a case, they may be retrieved by a personal identifier. For example, emails can be searched for by From:, To:, Cc:, and Bcc: addresses, which are indexed as fields in the eD2.0 Recommind system. The eD2.0 Recommind system attempts to index all document contents and metadata as text. Text searching then can be used to search for individual names and other personal identifiers.

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?

Recommind is used to search, review, and organize thousands of documents received by the SEC in the course of examinations, investigations, and litigation and manage case files. The primary privacy risks are that information collected is based on erroneous, inaccurate, untimely or incomplete data; decisions affecting the individual concerned may be made using irrelevant information; and users may use the information in ways that are inconsistent or beyond the scope of the information collection. Given the nature of investigatory material, it is not always possible to obtain accurate, relevant, timely and complete information. The SEC has exempted certain materials from the Privacy Act's access to records rule, as noticed by SEC-42. SEC personnel research materials and conducting the proper due diligence before taking an adverse action against an individual.

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	☒ 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?

The primary use of the data is for purposes of conducting examinations, investigations, and litigation. Information is used to gather facts in order to determine whether any person has violated, is violating, or is about to violate any provision of the federal securities laws or rules for which the Commission has enforcement authority. Additionally the data may be used for any of the routine uses as set forth in SORN SEC-42.

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

☒ SEC Employees
Purpose: User IDs are maintained in the system for internal auditing purposes.

☒ SEC Federal Contractors
Purpose: User IDs are maintained in the system for internal auditing purposes.

☒ Interns
Purpose: User IDs are maintained in the system for internal auditing purposes.

☒ Members of the Public
Purpose: Information is collected from individuals and entities outside the SEC in the course of Enforcement investigations.

☐ 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.

Enforcement Data Delivery standards (available publicly on https://www.sec.gov/divisions/enforce/datadeliverystandards.pdf) provide instructions to outside parties on how to provide information to the SEC, including how to protect the information. Enforcement voluntary document requests and subpoenas describe the information to be provided in each investigation. Enforcement investigative information is not used for testing, training, or research.

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

☐ No.

☒ Yes.
The NARA approved records schedule for Enforcement's investigative case files is NI-266-09-004.

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

Enforcement investigative case files are collected and transferred to Enforcement Records Management during the case closing process. Enforcement Records Management is in the process of determining how to implement the criteria for designating landmark and non-landmark cases. Retention period and disposition depend on whether a case is designated landmark or non-landmark.

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?

The primary risk is inadvertent or unauthorized disclosure of PII. This risk is mitigated by implementing access controls to limit access to those staff with a need to know. There is also a risk that sensitive information related to Enforcement investigations could be maintained for a period longer than necessary to achieve the agency's mission. Although there is always a risk inherent in retaining personal data for any length of time, the data retention periods based on case type identified in the NARA schedules are consistent with the concept of retaining personal data only for as long as necessary to support the agency's mission. Additionally, the information contained in Recommind is protected from unauthorized access through appropriate administrative and technical safeguards, which include access controls and encryption. Secure web protocols are used to encrypt data in transit. Secure file transfer methods encrypt transmissions among SEC Headquarters and the Regional Offices. Hardware encrypted media are used to transfer data externally.

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
Privacy Act notices, including Form 1661 and Form 1662, are included in Enforcement subpoenas and voluntary document requests.

☒ System of Records Notice
SEC-42, Enforcement Files

☒ Privacy Impact Assessment
Date of Last Update: 4/24/2012

☐ Web Privacy Policy

☐ Other notice:

☐ 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 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 material and often times 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 provide transparency by publication of this PIA and SORN-SEC-42.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

eD2.0 Recommind will group together documents with similar characteristics and this may reveal previously unrecognized issues and patterns. Keyword searching, Boolean searching, filtering, phrases, concept groups, email threading, and cluster diagrams are tools available within eD2.0 Recommind for attorneys to use in the course of investigations and to develop cases against potential wrongdoers. Filtering can be based on dates, organizations (producing party), domain names, email address, and other document metadata. The outcomes of

the data analysis may lead to new or broadened investigations of previously unknown patterns or concerns and could lead to additional enforcement actions and/or to additional document requests.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: Enforcement investigative teams have access to the data. Enforcement may share information with other SEC Divisions and Offices to use their expertise during investigations and litigation. However, this usually does not require sharing PII as each Division or Office has their own pod of Recommind. A pod is a master server and a set of other virtual servers to make a functioning Recommind system. For scalability and capacity management ENF is split up across 3 pods. ENF, OGC, OCIE and OIG have separate pods and separate administration protocols. Storage works at two levels in Recommind. The indexes for cases in Recommind are partitioned by pod, and not shareable between pods. The indexes include the searchable text of the documents and pointers to the actual document files. The document files are on large pools of network attached storage which are shared, but which are only accessible by the Recommind service accounts (not by regular user accounts).
Having separate pods with the storage managed as it is prevents one Office from accessing any information (PII or not) in another Office's pod. Separate pods reduce the impact of unauthorized disclosure, because if one pod is compromised, data in the other pods still is protected.

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

The primary privacy risk with internal sharing is inadvertent or unauthorized disclosure of sensitive PII. This risk is mitigated by implementing strict access controls limiting access to those staff with a business need. Additionally, SEC maintains separate instances or "pods" of Recommind for SEC divisions and offices outside of Enforcement. Separate pods reduce the impact of unauthorized disclosure because if one pod is compromised, data in the other pods still is protected. Finally, authorized SEC users are trained to recognize and protect the PII and other sensitive data likely to be available in the system.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: Documents are sometimes shared with other law enforcement agencies, and are produced to opposing counsel during litigation. The documents are transmitted on encrypted external media, or through secure file transfer methods. eD2.0 Recommind does not interconnect or share data with any system external to the SEC.

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

The primary privacy risk associated with external sharing is the risk of disclosure to unauthorized recipients during the transmission of information to external entities. The SEC minimizes this risk by ensuring that electronic transmissions are secured by encryption. The eD2.0 application has implemented SSL/TLS to encrypt confidential data sent over an intranet, it implements https protocol which encrypts the entire session between the client and the server and allow mutual authentication. Documents are transmitted on encrypted external media or through secure file transfer methods. Enforcement reviews productions before they are sent out to

ensure they do not contain whistleblower identifying information, suspicious activity reports or other Bank Secrecy Act information.

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): The Enforcement Division may receive information from many sources during an investigation. Enforcement 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. For example, an investigation into a corporation often leads to identify a few key document custodians. Responsive, non-privileged email and other documents in the possession, custody or control of the custodian are then provided to the SEC. Depending on the circumstances, documents may be provided directly by an individual or by the individual's corporate employer. As another example, investigations into trading activity often lead to account and transaction information being provided to the SEC by banks and broker-dealers.

6.2 What methods will be used to collect the data?

Documents are received by the SEC on external media, by file transfer and as attachments to email. Data Delivery Standards (available publicly on https://www.sec.gov/divisions/enforce/datadeliverystandards.pdf) instruct outside parties to encrypt sensitive data when providing it to the SEC.

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

The SEC maintains chain of custody records for the documents to demonstrate how they were received and processed. The accuracy of the documents and data is verified through testimony and litigation. The information received in the original correspondence is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise.

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

☒ No

☐ Yes.

System(s):

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 include that information collected is based on erroneous, inaccurate, untimely or incomplete data. This risk is mitigated by 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.

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.

Given the nature of the materials, individuals may not have notice as to whether their information was collected as part of an investigation. Individuals do not have the opportunity and/or right to decline to provide data and do

not have the right to consent to particular uses of the data. The law enforcement exception in the Privacy Act applies.

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

Although individuals may request access to information about themselves contained in a SEC system of records through the SEC Privacy Act/Freedom of Information Act (FOIA) procedures, Enforcement records are exempt from the access and correction provisions of the Privacy Act (see SORN SEC-42 "Enforcement Files").

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 PA and therefore access to such records will be restricted.

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 Recommind 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 compiled for law enforcement purposes. This risk is mitigated by SEC personnel researching materials; conducting the proper due diligence before taking an 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.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes
SA&A Completion Date: 2/6/2019
Date of Authority to Operate (ATO) Expected or Granted: 2/6/2019
☐ No

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

☒ Users
Roles: Enforcement, OCIE, OGC, OCR, and OIG staff attorneys, examiners, investigators, paralegals, and accountants performing investigations and conducting litigation
☒ Contractors
Roles: Supporting contractors loading data into eD2.0 Recommind and producing data from it
☐ Managers
Roles:
☐ Program Staff
Roles:
☐ Developers
Roles:
☒ System Administrators
Roles: Operating and maintaining the eD2.0 Recommind system
☐ Others:
Roles:

8.3 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

8.4 How will the system be secured?

The eD2.0 Recommind architecture consists of data source crawlers, index engines, meta-engines, and application servlets. Data source crawlers connect to data sources on the SEC network. Typically, the data sources are from external systems and require a manual process to load the data onto the SEC network.

The system integrates with active directory. UserID and password are required to access eD2.0 Recommind. Access to each case is controlled by an active directory security group and use of secure socket layer (SSL) for accessing the system over the internal SEC network.

Authorized users access Recommind through Citrix and over the SEC WAN. Recommind virtual servers run on physical hardware that is centrally located in the OIT data centers.

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

☒ No
☐ Yes
Public
URL:

8.6 Does the site have a posted privacy notice?

☐ No
☐ Yes
☒ N/A

8.7 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

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

There exists a risk of inadvertent or unauthorized disclosure. This is mitigated through the use of security groups for access control and https/ssl for communication. Additionally, the system is only accessible through a SEC connected network.

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.

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

☒ No
Reports generated by this system do not focus on the content of the individuals' data potentially contained within the system. For example, a report might indicate "Number of documents tagged Responsive" or "Types of documents added to workspace for Production

☐ Yes

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

Recommind software logs system activity. Analysis and audits of these logs are done for troubleshooting, analysis of system usage, and to determine who viewed or acted on specific documents in the system.

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?

Auditing and review of audit logs is performed according to the SEC's internal System Security Plan. Logging includes accessing the system, which is reviewed at least quarterly under this plan. The access log review will identify unauthorized or inappropriate access to data in the eD2.0 Recommind system. The SEC's Recommind environments are also routinely monitored for suspicious or malicious use activities including (but not limited to) checks on file share access, multiple failed login attempts, log file manipulation, unusual document tagging, and exports by non-approved users.

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.

Unauthorized access or inadvertent disclosure of information from the eD2.0 Recommind system could compromise Enforcement investigations or litigation, resulting in less enforcement of securities laws and regulations.