U.S. Securities and Exchange Commission

eD3 Casepoint Cloud Pilot
PRIVACY IMPACT ASSESSMENT (PIA)

August 21, 2020

Division of Enforcement

Privacy Impact Assessment

eD3 Casepoint Cloud Pilot

Section I: System Overview

1.1 Name of Project or System

eD3 Casepoint Cloud Pilot

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally hosted (Contractor or other agency/organization): Infotrends/Casepoint

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

The primary objective of the eD3 Casepoint Cloud Pilot is to assess a cloud-based electronic discovery (eDiscovery) platform as a replacement for the current eD2 Recommind Axcelerate platform. eD3 is 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. The platform employs a Software as a Service (SaaS) offering by Casepoint and provides enterprise-class tools for full-spectrum eDiscovery, including data processing, advanced analytics, artificial intelligence, and customizable productions that are created to share case data with outside parties. An outside party could be an individual, a Federal agency, an expert witness, or opposing counsel if a case were to go to trial.

eD3 supports terabytes of data which includes workflows across thousands of legal matters and millions of documents. The SEC uses eD3 Casepoint SaaS as a centrally managed repository for data and documents received from examinations, investigations, litigation, and Freedom Of Information Act (FOIA) requests. Casepoint enables users to easily search and review thousands of documents effectively and efficiently. The Division of Enforcement (ENF) uses Casepoint to manage complex litigation and the Office of Compliance Inspections and Examinations (OCIE) uses it to review data generated during the course of an exam. Attorneys and accountants search and organize documents in eD3 Casepoint to build their cases and prepare to take testimony. eD3 Casepoint does not share information with other systems.

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 and 17 CFR § 202.5

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:	The SSN is not requested but may be contained in examination, investigation, and litigation information sent to the SEC.
If yes, provide the legal authority:	15 U.S.C. §§ 77s, 77t, 78u, 77uuu, 80a-41, and 80b-9, 17 CFR § 202.5, and EO 9397, as amended

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

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?

Information is collected in the eD3 Casepoint Cloud Pilot to serve as a repository for examinations, investigations, and litigation data. The privacy risks are as follows: 1) information collected may be erroneous, inaccurate, untimely, or incomplete due to its investigatory nature; 2) decisions affecting the individual concerned may be made using inaccurate or incomplete information; and 3) users may use the information in ways that are inconsistent or beyond the scope of the purpose for which the information was collected.

Given the nature of investigatory material, it is not always possible to obtain accurate, relevant, timely, and complete information. However, SEC personnel research materials and conduct proper due diligence before taking any adverse action against an individual. As noticed by SORN SEC-42, the agency has exempted certain materials from the Privacy Act's access to records rule.

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: Documents containing additional identifying numbers may be submitted after a subpoena is issued, and this data, which is outside of SEC control, may be ingested.

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: Documents containing additional general personal data may be submitted after a subpoena is issued, and this data, which is outside of SEC control, may be ingested.

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: Click here to enter text.

Distinguishing Features/Biometrics

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

☐ Other: Click here to enter text.

System Administration/Audit Data

☒ User ID	☒ Date/Time of Access	☐ ID Files Accessed
☒ IP Address	☒ Queries Run	☐ 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?

Personally identifiable information (PII) is collected to support examinations, investigations, and litigation and 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 SEC has enforcement authority. Additionally, PII 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: The system maintains User IDs for internal auditing purposes.

☒ SEC Federal Contractors
Purpose: The system maintains User IDs for internal auditing purposes.

☒ Interns
Purpose: The system maintains User IDs for internal auditing purposes.

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

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

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

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

An Authorization to Test (ATT) was approved by the SEC Chief Technology Officer (CTO) to allow Casepoint to use PII within the eD3 pilot on 01/21/2020. Pursuant to this ATT, ENF was granted permission to migrate ten (10) closed cases (originating from Recommind) to the eD3 Cloud Pilot (Casepoint in Azure).

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

☒ No.
The information stored in the eD3 Casepoint Pilot is not categorized as federal records and there is no associated NARA retention schedule.

☐ Yes.
If yes, provide the retention period and cite to the NARA schedule.

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

At the end of the pilot, data will be disposed of as per data deletion standard operating procedures for the eD3 Pilot.

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?

The primary risk is potential 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. The information contained in eD3 Casepoint is protected from unauthorized access through appropriate administrative and technical safeguards, which include role based access controls and encryption. The application has user roles, and all data is segregated by case/matter. Secure web protocols are used to encrypt data in transit. Secure file transfer methods encrypt transmissions among SEC Headquarters, the Regional Offices, and the Azure cloud. In addition, 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 Forms 1661 and 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:
This PIA

☒ Web Privacy Policy
There is a link to the SEC privacy policy after SEC employees and affiliates log in to the Casepoint portal from a whitelisted IP address.

☐ Other notice:
What type of notice was provided? Where was the notice provided?

☐ 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 these 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, the individuals whose information may be found in the documents are sometimes not the providers of the information. However, the SEC has taken steps to provide transparency through publication of this PIA and SORN SEC-42.

Section 5: Limits on Uses and Sharing of Information

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

Users can quickly and easily organize documents through the use of tags, annotation of transcripts, reports, and complex search queries. Depending on the type of documents received for a given case, they may be retrieved through use of a personal identifier. For example, emails can be searched via "From:", "To:", "Cc:", and "Bcc:" addresses, which are indexed as fields in the eD3 Casepoint system. The eD3 Casepoint 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. eD3 Casepoint groups together documents with similar characteristics. The results 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. Keyword searching, Boolean searching, filtering, phrases, concept groups, email threading, and cluster diagrams are tools available within eD3 Casepoint for attorneys to use in the course of investigations and to develop cases against potential violators. Filtering can be based on date, organization (producing party), domain name, email address, or other document metadata.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: Examination and enforcement investigative teams have access to the data. ENF and OCIE may share information with other SEC Divisions and Offices to use their expertise during examinations, investigations, and litigation.

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 strict access controls limiting access to those staff members with a business need. Authorized SEC users are trained to recognize and protect the PII and other sensitive data likely to be resident in the system.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: In some cases, documents are shared with other law enforcement agencies and are provided to opposing counsel during litigation. The documents are transmitted on encrypted external media or through secure file transfer methods.

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 potential 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 eD3 Casepoint application encrypts confidential data sent over an intranet. It also implements "https" protocol, which encrypts the entire session between the client and the server and allows mutual authentication. Documents are transmitted on encrypted external media or through secure file transfer methods. ENF reviews Casepoint data before it is sent out, to other parties, to ensure whistleblower identifying information, Suspicious Activity Reports (SAR), or other Bank Secrecy Act (BSA) information is not disclosed.

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 receives 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 multiple individuals or branches of a corporate entity. For example, an investigation into a corporation often leads to identification of 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 email attachments. SEC Data Delivery Standards 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): If yes, list system(s). For each listed system state the purpose of the interaction.

6.5 Considering the sources of the data and methods of collection, what is the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

The primary privacy risk is that information collected may be 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 by verifying the accuracy of the documents and data through testimony and litigation.

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 will allow individuals to access their information?

Although individuals may request access to information about themselves contained in an SEC system of records through the SEC Privacy Act/Freedom of Information Act (FOIA) procedures, ENF 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?

Individuals may request access to and correction of their information under the SEC FOIA/Privacy Act procedures. However, access to such records will likely be restricted, as the data may be exempt from access and correction provisions of the Privacy Act.

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 which are available in the eD3 Casepoint system, there is a risk that inaccurate or erroneous information about an individual could be used by SEC personnel. This risk is mitigated by SEC personnel researching materials; conducting proper due diligence prior to initiating 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. This system is exempted from the Privacy Act insofar as it contains investigatory materials compiled for law enforcement purposes.

Section 9: Accountability and Auditing

8.1 Describe what privacy training is provided to users, either generally or specifically relevant 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 protection of PII.

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

☒ No
☐ Yes

If yes, describe how the reports or data extracts are secured. Describe the retention and disposal procedures for the data extracts or reports.

8.3 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

8.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes

Following events are logged for auditing:

1. User login and log off
2. Change of user permissions
3. Creating, modifying, deleting of user accounts

4. Changing user permissions
5. Accessing a case
6. Accessing a document
7. Importing of documents
8. Exporting of documents

8.5 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 eD3 Casepoint system could compromise ENF investigations or litigation, resulting in less enforcement of securities laws and regulations. The residual risk is low due to security controls in place.