U.S. Securities and Exchange Commission

eD3 Casepoint
PRIVACY IMPACT ASSESSMENT (PIA)

March 6, 2025

Division of Enforcement

Publication History

Revision	Date	Changes Made
Initial	03/30/2020	Original Document
1	06/09/2020	Review and Update
2	08/27/2024	Review and Update
3	03/06/2025	Updated for compliance with E.O. 14168

Section I: System Overview

1.1 Name of Project or System

eD3 Casepoint

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: 03/30/2020

Last updated: 03/06/2025

Description of update: Updated for compliance with E.O. 14168

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

eD3 Casepoint is a cloud-based electronic discovery (eDiscovery) platform replacing the retired eD2 Recommind Axcelerate platform. Casepoint is a Software as a Service (SaaS) 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. In addition, Casepoint 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.

The Division of Enforcement (ENF), the Office of Credit Ratings (OCR), the Division of Examinations (EXAMS), the Office of General Counsel (OGC), and the Office of Inspector General (OIG) use Casepoint for eDiscovery and to manage complex litigation and review information generated because of an exam. In addition, OIG uses Casepoint as a repository for data and documents received from examinations, investigations, litigation, and Freedom of Information Act (FOIA) requests. Attorneys and accountants search, review and organize documents in Casepoint to build cases and prepare testimony.

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, EO 9397, as amended, and the Inspector General Act of 1978, as amended (5 U.S.C. § 401 et seq.).

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 or collected from other internal sources.
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, and the Inspector General Act of 1978, as amended (5 U.S.C. § 401 et seq.).

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-04, Office of General Counsel Working Files, [85 FR 85440, January 27, 2021]

SEC-17, Enforcement Files [85 FR 85440, January 27, 2021]

SEC-18 Office of Inspector General Working Files [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?

Information is collected in Casepoint for examination. investigation, and litigation purposes. Privacy risks are: 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) information may be used in ways that are inconsistent or beyond the scope of the purpose for which the information was collected. To minimize these risks, authorized attorneys perform due diligence, including review of information collected before taking any adverse action against an individual. Information collected is used in accordance with the routine uses identified in the SORNs identified in section 2.4. In addition, court seals and legal safeguards, such as clawback agreements, are used when necessary.

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
☒ 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: 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 to address inquiries from members of Congress, the Government Accountability Office, or other entities responsible for monitoring the work of the Commission.

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. Information may also be used for OIG and OGC cases and investigations.

☒ SEC Federal Contractors
Purpose: The system maintains User IDs for internal auditing purposes. Information may also be used for OIG and OGC cases and investigations.

☒ Interns
Purpose: The system maintains User IDs for internal auditing purposes. Information may also be used for OIG and OGC cases and investigations.

☒ Members of the Public
Purpose: Information is collected from individuals and entities outside the SEC during EXAMS and OCR examinations and ENF, OGC, and OIG investigations and litigation.

☒ Employee Family Members
Purpose: Information may be used in OIG and OGC cases and investigations.

☒ Former Employees
Purpose: Information may be used in OGC and OIG cases and investigations.

☒ Job Applicants
Purpose: Information may be used in OGC and OIG cases and investigations.

☐ Vendors
Purpose: Information may be used in OGC and OIG cases and investigations.

☐ Other:
Purpose:

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

PII may be contained in the documents used for testing. Copies of real data are used to adequately test functionality. Testing is performed in the same overall cloud environment as the production system, but with access restricted to testers and system administrators. PII is minimized by collecting only information that is necessary to investigate allegations of criminal, civil and administrative violations.

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

No.

☒ Yes.
DAA-0266-2018-0002 Office of Inspector General Records

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

Most documents in eD3 Casepoint are non-record third party productions. These are deleted after the case is closed and any outstanding FOIA requests and legal holds are resolved. However, documents determined to be Federal records are retained as follows:

- Investigative Case Files of Historical Value, Final Reports of Audits, Evaluations and Studies, Significant Litigation Case Files are permanent. Closed cases are cut off at the end of the fiscal year in which the case closed and are then transferred to the National Archives fifteen (15) years after cutoff.

- Routine Investigative Case Files, Files Not Resulting in the Establishment of a Formal Case File, Audits Evaluations and Studies Supporting Records and Background Materials, are temporary. Closed cases are cut off at the end of the fiscal year in which the case closed and are destroyed ten (10) years after cutoff.

- Other Litigation Case Files, Legal Opinions, Reviews and Guidance are temporary and are cutoff at the end of every fiscal year and are destroyed ten (10) years after cutoff.

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 privacy risk related to the information collected 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. In addition, encryption is employed to protect information from unauthorized disclosure.

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-17 Enforcement Files
SEC-04 OGC Working Files
SEC-18 Office of Inspector General Working Files

☒ Privacy Impact Assessment
Date of Last Update: 08/21/2020

☒ Web Privacy Policy
Posted on the Casepoint portal home page

☒ Other notice:
When collecting information from individuals voluntarily, OIG personnel provide verbal notice regarding collecting information voluntarily.

☐ 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?

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 other privacy information including the SORNs identified in section 2.4.

Section 5: Limits on Uses and Sharing of Information

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

Methods used to analyze data include the use of tags, annotation of transcripts, reports, and complex search queries. Depending on the type of documents received for a given case, information retrieved may be retrieved for analysis using a personal identifier. In addition, Casepoint indexes all document content and metadata as text. Text searching then can be used to search for individual names and other personal identifiers. 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 during 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: EXAMS, ENF, and OGC investigative teams have access to the data and may share information with other SEC Divisions and Offices to use their expertise during examinations, investigations, and litigation. OGC may grant limited access to specific cases or subset data of a case on an 'as required' basis. This requirement could extend to any staff member (not organization) in SEC who is authorized access by the case's supervising attorney.

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

The risk to privacy risk from internal sharing is unauthorized disclosure of PII. This risk is mitigated by sharing information as described in section 5.2.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: When required, documents are shared with law enforcement agencies. In addition, and information may be provided to opposing counsel during litigation.

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

The risk to privacy risk from external sharing is disclosure to unauthorized recipients during the transmission of information to external entities. The SEC minimizes this risk by encrypting data in transit. In addition, authorized ENF personnel reviews Casepoint data before it is sent out 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, OGC, and OIG may receive information from many sources during an investigation. Information may be provided in 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 results in 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, email, interviews, and subpoena.

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 related to sources of data and collection method 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. Additionally, information about an individual is collected directly from the individual when feasible.

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.

Casepoint is exempt from the Privacy Act because it contains investigatory materials compiled for law enforcement purposes. Therefore, in general, individuals do not have the opportunity to decline to provide data or the right to consent to uses of the data. However, for limited situations, individuals may consent or decline to provide voluntary information for certain matters in accordance with SEC SORN-04 and SEC Forms 1661 and 1662.

7.2 What procedures will allow individuals to access their information?

Since Casepoint is exempt from the Privacy Act, individuals cannot access their information unless otherwise specified in SEC SORN-04 and SEC Forms 1661 and 1662.

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

Individuals under investigation may not amend information about themselves in the system and are exempt from the Privacy Act. Information provided voluntarily may be amended by submitting a written request to 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.

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

Given that individuals are not permitted to access or correct records about themselves, 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.

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 online collection of personal data?

☒ No
☐ Yes

Public URL: Click here to enter text.

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 generally or specifically relevant 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

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

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.

Unauthorized access or inadvertent disclosure of information 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.