U.S. Securities and Exchange Commission

Palantir Enterprise Data Analytics Platform (EDAP)

PRIVACY IMPACT ASSESSMENT (PIA)

March 6, 2025

Division of Enforcement

Publication History

Revision	Date	Changes Made
Initial	2/6/2014	Original Document
1	3/18/2014	Review and Update
2	6/4/2021	Review and Update
3	3/6/2025	Updated for compliance with E.O. 14168

Privacy Impact Assessment

Palantir Enterprise Data Analytics Platform (EDAP)

Section I: System Overview

1.1 Name of Project or System

Palantir Enterprise Data Analytics Platform (EDAP)

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: 2/6/2014

Last updated: 6/4/2021

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

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 Palantir Enterprise Data Analytics Program (EDAP) is an enterprise wide single-platform analytic software tool that provides the SEC the capability of integrating structured, unstructured, and semi-structured data. The SEC's Division of Enforcement and Division of Examinations utilize EDAP to find, analyze, and visualize connections between disparate sets of data, which assists in generating leads, identifying schemes, and uncovering fraud. Specifically, EDAP supports investigations into securities and related fraud, supports inspection of regulated entities, informs SEC policy development related to financial sector oversight, and assists with reporting requirements to ensure sufficient information is collected to support analysis.

EDAP aggregates duplicative information from several major SEC systems and combines this information for analysis. EDAP users can run queries to return data uniquely relevant to an investigation and/or examination and use identifiers to uncover previously unknown relationships and links between entities and individuals. These relationships can be used to evaluate leads and SEC's work. End users can export the results of their analysis through PowerPoint, Excel, HTML and GIS data. All of these activities are logged by the application. Information flow within EDAP is strictly controlled based on the level of access permitted to each user and all access to data sources is on a read-only basis.

EDAP enhances SEC effectiveness and efficiency by enabling users to assess data quickly and thoroughly, using built in product capabilities that reflect the investigative process across common case types. For example, EDAP has a chronology capability that allows investigators and examiners to create a timeline of activities/events. EDAP users can create a chronological sequence of events to generate visualizations and artifacts based on the data. The system does not alter data in any way, but simply copies it from other systems for comprehensive analysis. The application is not available externally. EDAP processes data from the following.

Systems:

- Enterprise Data Warehouse (EDW)
- Bluesheets as a Service_external (BSS)
- Investor Response Information Systems (IRIS)
- Tracking and Reporting Examination National Documentation system (TRENDS)
- eD2.0 Recommind Axcelerate (ED20)
- Enforcement Case Management (HUB)
- Tips, Complaints, and Referral system (TCR)
- Electronic Data Gathering, Analysis, and Retrieval system (EDGAR)

Datasets:

- FINRA Datamart and its subset, Form ADV
- Thomson Reuters M&A
- Over-the-Counter (OTC) Markets

- Wharton Research Data Services (WRDS), both Compustat and Center for Research in Security Prices (CRSP)

Additionally, investigators may load case-specific data that may include CLEAR reports, phone records, and disaggregated trade data.

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

15 U.S.C. 77a et seq., 78a et seq., 80a-1 et seq., 80b-1 et seq., and 5 U.S.C. 302.

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:	EDAP utilizes SSNs from Bluesheets to cross-match individuals across the data sources.
If yes, provide the legal authority:	SSNs are collected, pursuant to Section 21(a) of the Exchange Act and related rules authorizing the Commission to conduct investigations of potential violations of the federal securities laws, to identify such persons accurately, and assist in determining involvement in other matters.

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

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

☒ No
☐ Yes

EDAP does not meet the definition of an information collection and does not collect information from ten or more members of the public.

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

EDAP aggregates data from several SEC source systems to find, analyze, and visualize connections between disparate sets of data. The primary privacy risk related to the purpose of the collection is using information provided for one purpose inappropriately.

This risk is 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
☒ 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:		

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?

Information is collected, used, shared and maintained by EDAP to find, analyze, and visualize connections between disparate sets of data, to generate leads, identify schemes, undercover fraud, and for other related investigative activities.

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

☒ SEC Employees
Purpose: EDAP does not collect information on SEC employees, but does collect user account information.

☒ SEC Federal Contractors
Purpose: EDAP does not collect information on SEC federal contractors, but does collect user account information.

☒ Interns
Purpose: EDAP does not collect information on SEC interns, but does collect user account information.

☒ Members of the Public
Purpose: EDAP collects information on Members of the Public from the data sources cited in Section 2.1 to enable analysts to perform data analyses.

☐ Employee Family Members
Purpose:

☐ Former Employees
Purpose:

☐ Job Applicants
Purpose:

☐ Vendors
Purpose:

☒ Other: Palantir Contractors
Purpose: EDAP does not collect information on Palantir contractors, but does collect user account information.

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

Palantir EDAP is a data integration platform for 12+datasets. To ensure that system testing occurs in an environment that accurately represents the Production environment, a large subset of the Production environment data, which includes PII and non-public information, will be used for testing in the stage environment. The integration is intended to ensure different types of data interact with one another and are performant at scale. Access to the data in the stage environment is limited to approximately six EDAP administrators (Palantir contractors) and two test accounts for OIT Security Penetration testers, in order to test new periodic releases. The stage environment data may also be exposed to each respective end users for the temporary purpose of testing the new EDAP functionality in the Staging environment prior to

Production release in coordination with EDAP's OIT and business sponsors. PII is not used for training or research efforts.

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

☒ No.

EDAP only captures duplicative reference material, not data that is defined as a record per the Federal Records. Any unique record material that is needed in support of and investigation will be maintained by ENF in the appropriate case file.

☐ Yes.

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

EDAP is not the official repository for any documents or data, rather EDAP is a platform that provides ENF and The Division of Examination (EXAMS) staff with a network infrastructure to better perform their jobs. At the conclusion of the contract, Palantir is responsible for archiving and returning all remaining SEC data to the contracting officer representative (COR) and disposing of data in accordance with NIST SP 800-88.

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 privacy risk relating to the type of information collected is risk of inadvertent or unauthorized access/disclosure of nonpublic information.

To mitigate these risks, the system leverages AD for authentication to mitigate the potential for unauthorized access of data. Information flow within EDAP is strictly controlled based on the level of access permitted to each user and all access to data sources is on a read-only basis. Once the user is added to the AD group, they are able to log in to the application; however the data they can see is dictated by the AD groups used by the source-data application. The EDAP system has detailed audit and accountability procedures to ensure that actual data access conforms to authorized use of the system. All users are

required to take mandatory training on Cyber Security and Privacy Awareness, Protecting Nonpublic Information, and Records Management.

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

Since EDAP does not collect information directly from individuals and no new information is created though the system about individuals, any PII in EDAP will be collected from an existing SEC system and will be covered by a SORN listed below:

- SEC-17 ("Enforcement Files")
- SEC-25 ("Information Pertaining or Relevant to SEC Regulated Entities and their Activities")
- SEC-05 ("Office of Municipal Advisor Records")
- SEC-29 ("Tips, Complaints, and Referrals Records")
- SEC-31 ("Investor Response Information System")
- SEC-33 ("General Information Technology Records")
- SEC-01 ("SEC's Division of Corporation Finance Records")
- SEC-02 ("SEC's Division of Investment Management Records")
  SEC-03 ("SEC's Division of Trading and Markets Records")

☒ Privacy Impact Assessment
Date of Last Update: 3/18/2014

☐ 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 these risks mitigated?

The primary privacy risk is individuals may not know that SEC utilizes EDAP to analyze the data transmitted through other SEC systems and the outcomes of the data analysis may lead to new or broadened investigations or examinations of previously unknown patterns and concerns. This potential risk is mitigated by ensuring that SORNs are current and adequately cover all source system information and this PIA is updated and published.

Section 5: Limits on Uses and Sharing of Information

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

SEC users will use EDAP as a flow-through tool for network analysis, clustering, enterprise data sharing/collaboration. The outcomes of the data analysis may lead to new or broadened investigations of previously unknown patterns or concerns. The information collected about an individual or organization can be added to their existing investigation file/record or can lead to a new file being created. The information gleaned from data analysis, clustering, or network analysis could be used to take action against an individual identified in an investigation using EDAP. If a new investigation or exam is created, it can be made available to Government employees who could make determinations against that individual. EDAP has reporting capabilities with the data output easily shareable via file extracts, emails, or presentations. Information would only be shared on a strict need-to-know basis to authorized individuals. EDAP activity is auditable, so one can see who has access to data, when, and where it has been sent/shared.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: ENF and EXAMS

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

The privacy risk from internal sharing is unauthorized, inadvertent or unauthorized disclosure of nonpublic information to individuals without a need to know. There is a risk of a user downloading data and sharing it with users that do not have access to data, a risk of data files created for ingestion being available to personnel that have access to the servers but not the systems, and risks of users publishing data within the application for visibility for a broader audience that includes users that do not have access to the underlying systems.

These risks will be mitigated by the granular access controls built into EDAP (by group, user type, case type, and/or record type) to protect the data at all levels to only authorized users. Only authorized users will receive access to data within EDAP. Additionally, the system will employ audit capabilities to ensure system access and use is appropriate. All users are required to take mandatory training on Cyber Security and Privacy Awareness, Protecting Nonpublic Information, and Records Management.

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.

Privacy risks related to external sharing are minimal as external organizations will not have access to the data from the system. However, the SORNs delineate the permissible disclosure of the information from the original sources in the routine uses.

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): EDAP processes data from the several source systems, including ARTEMIS (ADAP)/EDW, Bluesheet Internal, Bluesheet FINRA, Investor Response Information Systems (IRIS), the Tracking and Reporting Examination National Documentation system (TRENDS), FINRA Datamart, Recommind, the HUB system, the Tips, Complaints, and Referral system (TCR), Electronic Data Gathering, Analysis, and Retrieval system (EDGAR), Thomson Reuters M&A, OTC Markets, and Wharton Research Data Services (WRDS), as well as case-specific data loaded by investigators which may include CLEAR reports, phone records, and disaggregated trade data. Data may be public (as in the case of much EDGAR data), obtained from a regulated entity such as an exchange or SRO (as in the case of some ABAP data), generated by the SEC (as in the case of HUB data and some TCR data), sent from the public voluntarily (as in the case of a tips or complaints) or produced in response to an administrative subpoena. EDAP users may also import data into the system to support individual research, examination, and investigative efforts.

6.2 What methods will be used to collect the data?

EDAP does not collect data directly from individuals, but rather it processes existing SEC data from various underlying source systems. For the majority of systems, EDAP will transmit the data by directly connecting to the source system's database and running a series of database queries. This will be done using EDAP data integration scripts, which utilize Java's Database Connectivity (JDBC), an application programming interface (API) for the programming language Java, which defines how a client may access a database. In the case of Recommind, which does not have an accessible database, file-based exports of the case data will be created which will in turn be read by the data integration scripts.

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

The data EDAP receives is presumed to be accurate, relevant, timely and complete. EDAP assumes, the originating source system validates the data for completeness.

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

☐ No

☒ Yes.

System(s): EDAP processes data from the several source systems, including ARTEMIS (ADAP)/EDW, Investor Response Information Systems (IRIS), the Tracking and Reporting

Examination National Documentation system (TRENDS), Bluesheet FINRA, Bluesheet Internal, FINRA Datamart, Recommind, the HUB system, the Tips, Complaints, and Referral system (TCR), Electronic Data Gathering, Analysis, and Retrieval system (EDGAR), Thomson Reuters M&A, OTC Markets, and Wharton Research Data Services (WRDS), as well as case-specific data loaded by investigators which may include CLEAR reports, phone records, and disaggregated trade data.

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 privacy risks related to data quality and integrity include use of information that is inaccurate or outdated. This potential risk is mitigated by a data integration process by which the EDAP system regularly connects to source systems and replaces or updates data as needed. The source system serves as the initial point of collection whereby individuals either directly provide information or a third party provides information about individuals. The EDAP system connects to source systems on a regular basis – nightly or weekly depending on the frequency by which the source system updates its data – to refresh the data in the EDAP system. Each data source is configured to check the source system for updates in a manner that is appropriate to the source system. For example, a relatively small source system is reviewed in full during each sync and data is updated or replaced appropriately. Data from larger source systems is ingested via the source's last modified date or similar attribute which identifies all data that needs to be updated in the EDAP system. This process ensures that data in the EDAP system reflects the same data that exists in the source systems.

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.

EDAP is a read only platform that integrates data from other systems of records. EDAP is not itself a system of record, cannot make changes to source system data and is not public facing. EDAP is an internal tool to the SEC. Any opportunities for individuals to decline to provide information or opt out would be conducted at the underlying source system level.

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.

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 may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736.

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

There is minimal risk related to individual participation. All EDAP records are covered by existing SORNs, which afford Privacy Act redress options. 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. Individuals are provided notice of procedures for participation and redress via applicable SORNs for the source information collection 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?

☒ Yes
SA&A Completion Date: 3/28/2017
Date of Authority to Operate (ATO) Expected or Granted: 3/24/2017

☐ No

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

☒ Users
Roles: Full access to system functionality without administrator rights

☒ Contractors
Roles: User, Admin (in the case of Palantir contractors)

☒ Managers
Roles: User

☒ Program Staff
Roles: User

☐ Developers
Roles:

☒ System Administrators
Roles: Full access to system functionality with administrator rights

☒ Others : Privileged Accounts
Roles: Operation system level accounts needed for system engineers are used to maintain the servers hosting the application.

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

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 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
☒ Yes

EDAP users have the ability to manually extract some data from the system for reporting and continued investigative use outside of the system. Those users are responsible for protecting that information according to SEC privacy protection policies. The system does not automatically generate reports.

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

The EDAP system is covered by detailed audit and accountability procedures. Individual user activity is logged for audit purposes includes system access, data queries, and data tagging.

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.

The expected residual risk related to access, given the sensitivity of the PII in the system, is that an authorized user may have more permissions than required to perform their job function. To mitigate this risk, authentication to the EDAP application is handled by the SEC AD. AD is configured to enforce a limit of three consecutive invalid access attempts by a user during a 15 minute time period, as well as automatically locking the account for fifteen minutes, when the maximum number of unsuccessful attempts is exceeded.

EDAP Linux server accounts have been configured to be compliant with SEC requirements. Server accounts are locked after 3 consecutive failed login attempts and are automatically unlocked after 15 minutes.

All SEC information systems must be configured to automatically timeout the session after a time period not to exceed 60 minutes, as documented in the SSP of inactivity. SEC workstations and laptops will time out after a period of 15 minutes of inactivity, which serves as a compensating security control for other applications, because their access is dependent upon network connectivity; Re-establishment of the session shall take place only after the user has properly authenticated.