# Executive Office for United States Attorneys (EOUSA)


## Privacy Impact Assessment
for the
USA Palantir Data Analytic Platform (USAPDAP)

Issued by:

Kevin Krebs

Senior Component Official for Privacy

Approved by: Peter Winn, Senior Agency Official for Privacy
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: May 21, 2025

*(March 2025 DOJ PIA Template)*

## Section 1: Executive Summary

The United States Attorneys' Palantir Data Analytic Platform (USAPDAP) is an electronic system that facilitates data analysis to support the Office of the Attorney General (OAG), Executive Office for United States Attorneys (EOUSA), and the United States Attorney's Offices (USAOs) investigations and litigation. The system allows authorized USAO trial attorneys, contract attorneys, paralegals, and analysts to support the following investigation and litigation functions: document review and triage, link analysis, case theory investigations, deposition preparation, and creation of trial exhibits. USAPDAP allows the investigation or trial team to share case data in a secure and collaborative environment and to limit access to data sets on a need-to-know basis.

EOUSA conducted this PIA to comply with the E-Government Act of 2002, the Federal Information Security Modernization Act, Department of Justice IT Security Standards and Security Authorization Process, and National Institute of Standards and Technology's NIST 800-53 Rev. 4. Based on these requirements, EOUSA has determined that USAPDAP maintains sensitive material, including information about individuals that is protected by various privacy statutes, regulations, and guidance. The personally identifiable information (PII) USAPDAP maintains is collected by EOUSA and the USAOs in the course of investigations and litigation in order to effectuate the Department's litigation mission.

## Section 2: Purpose and Use of the Information Technology

***2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.***

USAPDAP is a data integration and analysis platform that integrates data of any size or format, indexes and models the data into a unified format, and makes the data available for analysis using a variety of embedded applications and helpers. The system allows users to integrate data in different formats, analyze this data within a single compatible workspace, and produce analytic work products in a variety of formats. The system provides statistical analysis to identify trends, highlight outliers, and identify correlations in large-scale data sets.

Palantir software, including Foundry and the Artificial Intelligence Platform (AIP), enables a multitude of collaborative and operational workflows for end government users. USAPDAP is designed to help attorneys or other professional staff members acquire, organize, analyze and present evidence or other data as part of investigations and litigation. Through the use of computer data processing, image management, trial presentation systems, and other technologies, litigation materials are effectively

organized so that attorneys and other professional staff can rapidly locate information and make the best use of it in conducting an investigation, litigation, and settlement negotiation. USAPDAP will also assist with resource allocation in identifying litigation trends.

Palantir Foundry is a data integration and analytics tool used for data analysis, business intelligence (BI), and visualization within USAPDAP. It allows users to transform ingested data into readable dashboards to use as part of their decision-making processes.

The Artificial Intelligence Platform (AIP) within USAPDAP allows the OAG, EOUSA, and USAO users the ability to run summary reports of cases they are reviewing and litigating. AIP will enhance the OAG, USAO, and EOUSA's ability to parse case summaries and provide a quick and efficient overview of numerous cases in an expedited manner. The summary outputs will be used by OAG and EOUSA offices, including the US Attorneys and Assistant US Attorneys, to support criminal and civil investigations, as well as to prosecute or defend federal court cases including appellate cases. These outputs will inform decisions on investigative actions, legal processes, and litigation strategies, and help to understand litigation trends.

USAPDAP houses data collected in the course of civil and criminal investigations or litigation. The information may be collected as part of a law enforcement investigation or may be produced to DOJ by an opposing party in the course of the discovery process overseen by the federal courts. The information ingested into the system depends on the data provided to the DOJ for a specific case. It can include, but is not limited to, all types of sensitive, confidential business information, personally identifiable information (PII), or personal health information (PHI) collected in an investigation or produced in the discovery process. Publicly available information may also be incorporated if deemed relevant to the litigation. Publicly available information may include, but is not limited to, newspaper articles and other published journalism, public records, court records, social media information, and other data traditionally considered "open source."

Information in USAPDAP will come from case files stored in the USA Case Management Enterprise System (USACMES) CaseView application, the USAO case management system for civil and criminal investigations and litigation, and from PACER, via a connection between the Enterprise Application Development (EAD) Data Warehouse and USAPDAP. USAPDAP is made up of the Palantir Federal Cloud Service (PFCS) High Software as a Service (SaaS) solution, a dedicated environment for the purpose of delivering Palantir software to federal government customers as a cloud service, plus an on-premises Red Hat Enterprise Linux (RHEL) 9 server hosted in the EOUSA Network Operations Center (NOC). This server establishes the connection to USACMES to download the necessary case data and then sends it to the PFCS solution.

USAPDAP does not communicate with any external systems. USAPDAP is granted direct database access to specific case files in USACMES and information from PACER via the EAD Data Warehouse. This connection allows for bulk extract from the case file and integration of the data into USAPDAP. No information from USAPDAP is sent to

USACMES or PACER, and the extract setup is read-only, meaning USAPDAP does not modify, add, or delete data within USACMES or PACER. Built-in processes structure data upon ingest and automated checks are designed to ensure that data was technically ingested correctly and remains up-to-date.

The collaborative features integrated into USAPDAP's security model allow the maximum amount of information to be shared as authorized without leaking protected information. This secured sharing is accomplished by the "security-aware" functionality within the application. When users collaborate in USAPDAP, they are sharing a link and each are accessing the underlying data element directly (within the secured space of the application), not passing a copy of the information between users. When the recipient uses the shared link to view the data element, the recipient only sees the components of that item which the recipient has permission to view, if any.

All data and information within USAPDAP will be encrypted at rest and in transit. Access to the application will be limited to user authentication via USAauth (Okta), with permissions/roles based on least privilege. Additionally, access provisioning will utilize the USAidgov-gc workflow. USAidgov-gc is the EOUSA instance of Sailpoint, which supports automated lifecycle management for user accounts across the EOUSA enterprise—including application assignments and role entitlements. This allows for the automatic provisioning and de-provisioning of user accounts within USAPDAP via integration with USA Active Directory and USAauth.

Information in USAPDAP is only accessible to the OAG, USAO, and EOUSA offices of DOJ. All individuals with access to the data are cleared federal or contractor personnel.

***2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)***

| Authority | Citation/Reference |
|---|---|
| Statute | 28 U.S.C. §§ 514, 516, 517, 518, and 547 |
| Executive Order | |
| Federal regulation | 28 CFR § 0.45, Subpart I, et seq. |
| Agreement, memorandum of understanding, or other documented arrangement | |
| Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology

***3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed***

***by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.***

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |
| **Name** | X | A, B, C, D | Full name of individuals who are the subject of or otherwise identified in the underlying case. |
| **Date of birth or age** | X | A, B, C, D | DOB or age of individuals who are the subject of or otherwise identified in the underlying case. |
| **Place of birth** | X | A, B, C, D | Place of birth of individuals who are the subject of or otherwise identified in the underlying case. |
| **Sex** | X | A, B, C, D | Sex of individuals who are the subject of or otherwise identified in the underlying case. |
| **Race, ethnicity, or citizenship** | X | A, B, C, D | Race, ethnicity, or citizenship of individuals who are the subject of or otherwise identified in the underlying case. |
| **Religion** | X | A, B, C, D | Religion of individuals who are the subject of or otherwise identified in the underlying case. |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | X | A, B, C, D | SSN of individuals who are the subject of or otherwise identified in the underlying case. |
| **Tax Identification Number (TIN)** | X | A, B, C, D | TIN of individuals who are the subject of or otherwise identified in the underlying case. |
| **Driver's license** | X | A, B, C, D | Driver's license of individuals who are the subject of or otherwise identified in the underlying case. |
| **Alien registration number** | X | A, B, C, D | Alien registration number of individuals who are the subject of or otherwise identified in the underlying case. |
| **Passport number** | X | A, B, C, D | Passport number of individuals who are the subject of or otherwise identified in the underlying case. |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Mother's maiden name** | X | A, B, C, D | Mother's maiden name of individuals who are the subject of or otherwise identified in the underlying case. |
| **Vehicle identifiers** | X | A, B, C, D | Vehicle identifiers of individuals who are the subject of or otherwise identified in the underlying case. |
| **Personal mailing address** | X | A, B, C, D | Personal mailing address of individuals who are the subject of or otherwise identified in the underlying case. |
| **Personal e-mail address** | X | A, B, C, D | Personal e-mail address of individuals who are the subject of or otherwise identified in the underlying case. |
| **Personal phone number** | X | A, B, C, D | Personal phone number of individuals who are the subject of or otherwise identified in the underlying case. |
| **Medical records number** | X | A, B, C, D | Medical records number of individuals who are the subject of or otherwise identified in the underlying case. |
| **Medical notes or other medical or health information** | X | A, B, C, D | Medical notes or other health information of individuals who are the subject of or otherwise identified in the underlying case. |
| **Financial account information** | X | A, B, C, D | Financial account information of individuals who are the subject of or otherwise identified in the underlying case. |
| **Applicant information** | X | A, B, C, D | Applicant information of individuals who are the subject of or otherwise identified in the underlying case. |
| **Education records** | X | A, B, C, D | Education records of individuals who are the subject of or otherwise identified in the underlying case. |
| **Military status or other information** | X | A, B, C, D | Military status of individuals who are the subject of or otherwise identified in the underlying case. |
| **Employment status, history, or similar information** | X | A, B, C, D | Employment status or work history of individuals who are the subject of or otherwise identified in the underlying case. |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | X | A, B | Employment performance ratings can be included if a personnel termination case goes to litigation |
| **Certificates** | X | A, B, C, D | Certificates of individuals who are the subject of or otherwise identified in the underlying case. |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Legal documents** | X | A, B, C, D | Legal documents of individuals who are the subject of or otherwise identified in the underlying case. |
| **Device identifiers, e.g., mobile devices** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Web uniform resource locator(s)** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Foreign activities** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Criminal records information, e.g., criminal history, arrests, criminal charges** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Juvenile criminal records information** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Civil law enforcement information, e.g., allegations of civil law violations** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Whistleblower, e.g., tip, complaint, or referral** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Grand jury information** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Procurement/contracting records** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Proprietary or business information** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| **Location information, including continuous or intermittent location tracking capabilities** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| ***Biometric data:*** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| - **Photographs or photographic identifiers** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| - **Video containing biometric data** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| - **Fingerprints** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| - **Palm prints** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| - **Iris image** | | | |
| - **Dental profile** | | | |
| - **Voice recording/signatures** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| - **Scars, marks, tattoos** | X | A, B, C, D | This information may be included in case information and pulled into this system as part of the case file. |
| - **Vascular scan, e.g., palm or finger vein biometric data** | | | |
| - **DNA profiles** | | | |
| - **Other (specify)** | | | |
| ***System admin/audit data:*** | X | A | |
| - **User ID** | X | A | This information will be collected for DOJ employees accessing the system for the purpose of administering and auditing the system and use. |
| - **User passwords/codes** | X | A | This information will be collected for DOJ employees accessing the system for the purpose of administering and auditing the system and use. |
| - **IP address** | X | A | This information will be collected for DOJ employees accessing the system for the purpose of administering and auditing the system and use. |
| - **Date/time of access** | X | A | This information will be collected for DOJ employees accessing the system for the purpose of administering and auditing the system and use. |
| - **Queries run** | X | A | This information will be collected for DOJ employees accessing the system for the purpose of administering and auditing the system and use. |
| - **Contents of files** | X | A | This information will be collected for DOJ employees accessing the system for the purpose of administering and auditing the system and use. |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Other (please list the type of info and describe as completely as possible):** | X | A, B, C, D | Information pertaining to witnesses, confidential informants, and expert witnesses, as well as information pertaining to federal employees from other agencies that may be involved in litigation may be included. Other PII present in case files may also be included. Any other PII pertaining to reported security incidents or breaches may also be included. |

### *3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)*

| **Directly from the individual to whom the information pertains:** | | | | | |
|---|---|---|---|---|---|
| In person | X | Hard copy: mail/fax | X | Online | X |
| Phone | X | Email | X | | |
| Other (specify): Information collected during discovery may be collected from individuals who are opposing parties in the litigation. The request for such information would be through the discovery process overseen by the court. However, individuals do not directly input information into the system. | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | X | Other federal entities | X |
| State, local, tribal | X | Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer) | X | | |
| Other (specify): | | | | | |

| **Non-government sources:** | | | | | |
|---|---|---|---|---|---|
| Members of the public | X | Public media, Internet | X | Private sector | X |
| Commercial data brokers | X | | | | |
| Other (specify): | | | | | |

## Section 4: Information Sharing

### *4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual*

***secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.***

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Within the Component | X | X | X | USAPDAP receives an automated daily bulk transfer of data from CMES. Authorized users with a need-to-know will have direct log-in access. |
| DOJ Components | X | | X | Authorized users will have direct log-in access on a need-to-know basis. |
| Federal entities | | | | |
| State, local, tribal gov't entities | | | | |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | | | | |
| Private sector | | | | |
| Foreign governments | | | | |
| Foreign entities | | | | |
| Other (specify): | | | | |

***4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.***

N/A. No information from USAPDAP will be released to the public.

## Section 5: Notice, Consent, Access, and Amendment

***5.1 What kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.***

Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation. Notice may not be provided for information collected in the course of an investigation or other authorized law enforcement activity, including information that is considered publicly available, as doing so may jeopardize the investigation.

USAPDAP is covered by the following SORNs:

- USA-007, Criminal Case Files, last published in full at 53 Fed. Reg. 1864 (Jan. 22, 1988), available at https://www.justice.gov/opcl/docs/usa-007-53fr1864.pdf.
- USA-013, U.S. Attorney, District of Columbia Superior Court Division, Criminal Files, 54 Fed. Reg. 42097 (Oct. 13, 1989), available at https://www.justice.gov/opcl/docs/54fr42097.pdf.
- OAG-001, General Files System, 50 Fed. Reg. 37294 (Sep. 12, 1985), https://www.justice.gov/opcl/docs/50fr37294.pdf.

***5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.***

Individuals will not have the opportunity to voluntarily participate in the collection, use, or dissemination of their information in the system. Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation.

***5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.***

Individuals can submit a FOIA request to gain access to the information pertaining to them within USAPDAP. Information and resources for making a FOIA request are available at https://www.justice.gov/usao/resources/making-foia-request and https://eousafoia.usdoj.gov/.

## Section 6: Maintenance of Privacy and Security Controls

***6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).***

| | |
|---|---|
| X | **The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** March 20, 2025<br><br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br><br>**Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** No POAMs currently in place. |
| | **This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:** |
| X | **This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** USAPDAP has been categorized as a Moderate system. All applicable moderate baseline controls will be implemented and assessed accordingly. Any controls that are not implemented will be tracked for remediation in a POAM. |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** USAPDAP is the EOUSA instance of the Palantir FedRAMP High authorized Palantir Federal Cloud System (PFCS). EOUSA has conducted a baseline security evaluation of the system – assessment of compliance and vulnerability scans and encryption model and review of the FEDRamp documentation - and is undergoing a full assessment of the system controls now that the contract has been approved. This platform will utilize information from USACMES via the EAD, both of which have gone through full security assessments with the applicable controls. |
| X | **Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** System audit logs are reviewed on a weekly basis. USAPDAP is configured to send audit logs to USA-P-AAP (Splunk). |
| X | **Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. |

| | |
|---|---|
| | **Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** N/A |

***6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?***

The information maintained on USAPDAP is protected in accordance with applicable DOJ guidance, policies, and directives. USAPDAP exists on a physically secure, environmentally protected, DOJ network. The network is protected by firewalls and is administered by DOJ federal and contractor personnel. Access to USAPDAP is granted only to DOJ cleared and approved individuals who have signed a confidentiality agreement and system rules of behavior. Security training and a public-trust background check are performed on a regular basis on all staff who request access. Access to specific databases/folders/material is granted on a need-to-know basis by authorized Federal staff. Finally, all USAPDAP accounts are "named user" accounts assigned to a single individual and require PIV authentication via USAauth. Group, test, training, or temporary accounts are not permitted to accurately log the individual accessing the information. USAPDAP is configured to send audit logs to USA-P-AAP (Splunk), which are received and reviewed on a weekly basis.

***6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.***

Files managed on USAPDAP may include both federal records and non-records that are associated with a variety of different types of litigation case files. The retention policies for the files depend on the federal record status as well as the classification of the type of case file to which the files pertain. The Department of Justice record retention schedules are published at https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060.

Record retentions for case files range from approximately 5 years to 65 years after the case closure date. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration. Non-records are destroyed when no longer needed for convenience of reference.

USAPDAP utilizes the Artificial Intelligence Platform (AIP) that is part of the PFCS

FedRAMP package. However, USAPDAP information is restricted from being retained and used to train this AI model.

## Section 7: Privacy Act

***7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).***

_____ No. __X___ Yes.

***7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:***

- USA-007, Criminal Case Files, last published in full at 53 Fed. Reg. 1864 (Jan. 22, 1988), available at https://www.justice.gov/opcl/docs/usa-007-53fr1864.pdf.
- USA-013, U.S. Attorney, District of Columbia Superior Court Division, Criminal Files, 54 Fed. Reg. 42097 (Oct. 13, 1989), available at https://www.justice.gov/opcl/docs/54fr42097.pdf.
- OAG-001, General Files System, 50 Fed. Reg. 37294 (Sep. 12, 1985), https://www.justice.gov/opcl/docs/50fr37294.pdf.

## Section 8: Privacy Risks and Mitigation

***When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.***

As described above, the information contained in USAPDAP received in the course of an investigation or litigation. The documents are typically provided by another federal or state entity involved in the investigation or by the opposing party in the litigation in response to a subpoena or other discovery request. The privacy risks associated with collecting records from other entities is that they will share information outside the scope of the investigation or not properly identify the data being ingested into the system as containing personally identifying information. Preventing the exposure of the data once is it received by DOJ minimizes the risk that personal information will be shared outside the team of individuals working on a particular matter. To this end, DOJ places strict access controls on USAPDAP via physical and electronic means in order to secure the information.

An additional risk is the collection of inaccurate data. Data produced for the system may contain

errors. By allowing data from different sources to be analyzed in a single workspace while allowing multiple authorized users to review the data, the system facilitates the identification of inconsistencies that might indicate an error. Corrections to data are disseminated to all users within seconds of correction, and audit trails ensure that users are aware of the error and the correction.

Additional privacy risk mitigation efforts in place for USAPDAP include, but are not limited to:

- Allowing only a limited amount of data to be pulled into the system boundary.
- Restricting access to the information to internal, cleared DOJ users only.
- Restricting access to the system to DOJ network connected devices and users.
- Implementing robust encryption and access controls to safeguard sensitive data and prevent unauthorized access or breaches.
- Weekly audit log reviews to identify anomalous user access or activity.
- Ensuring that all AI applications comply with relevant privacy laws, regulations, and ethical guidelines, with particular attention to preventing overreach and safeguarding civil liberties.
- Ensuring that the data ingested by the AI is not retained or used to train the model.
- Providing training for staff on best practices for data handling, privacy protections, and the ethical use of AI to further reduce risks and maintain compliance.