Executive Office for U.S. Attorneys (EOUSA)

Privacy Impact Assessment
for the
USA Advanced Analytics Platform (USA-P-AAP)

Issued by:

Kevin Krebs

Senior Component Official for Privacy

Approved by: Christina Baptista, Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: May 29, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

The USA Advanced Analytics Platform (USA-P-AAP) is the EOUSA instance of Splunk Enterprise, the main security information and event management (SIEM) tool for the agency. USA-P-AAP system provides real-time data collection, monitoring and reporting across the DOJ EOUSA's enterprise solution infrastructure. The USA-P-AAP provides centralized audit log collection, review, analytics, and compliance dashboard views for all EOUSA/USAO systems.

The USA-P-AAP system enforces federal requirements for audit log review and analysis in accordance with OMB Memorandum M-21-31 to ensure that required baseline auditable events are being recorded, monitored, and responded to in the event of any anomalous activity for systems in on-premises or cloud hosted environments. All systems have a Splunk forwarder installed, or where this is not an option, will have their logs forwarded via syslog to the USA-P-AAP syslog server, to aggregate audit logs into an easy to view dashboard for automated log collection and review. This will achieve a goal of collaboratively facilitating security alerting, investigations, and response across the various CSS functions and between USA system owners and the Office of Chief Information Officer (OCIO).

USA-P-AAP additionally uses Security Orchestration, Automation, and Response (SOAR) and User Behavior Analytics (UBA) capabilities to provide automated monitoring, detection, correlation, and response capabilities to the EOUSA Security Operations Center (SOC), Insider Threat Prevention and Detection Team (ITPDT), and Network Operations Center (NOC).

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.

USA-P-AAP primarily serves as EOUSA's centralized audit logging repository for all operating system, database, and application-level logs for systems across EOUSA. System event, authentication, and object access logs for each authorized system are forwarded to USA-P-AAP Splunk instances, where they are then ingested into a web-based graphical user interface (GUI) where system personnel can access and review the logs to satisfy audit log collection and review requirements in support of OMB M-21-31.

USA-P-AAP is made up of several components, noted below:

Splunk Enterprise – Gives EOUSA the ability to search, analyze, and visualize the data from system components that are configured to forward application and device audit logs to the USA-P-AAP dashboard. Splunk Enterprise indexes the defined data and parses it

into a series of individual events that can be easily viewed and searched in the dashboard. This is the core component for the USA-P-AAP system and provides the backbone to provide OMB 21-31 compliance for EOUSA.

Splunk Enterprise Security – Provides additional insight into machine data generated from security technologies such as network, endpoint, access, malware, vulnerability, and identity information. It enables security teams to quickly detect and respond to internal and external attacks to simplify threat management while minimizing risk and safeguarding your business. This function is primarily used by the Security Operations Center (SOC) for incident response.

Indexer – Serves as the repository for Splunk Enterprise data. Splunk Enterprise transforms incoming data into events, which are stored in indexes on designated Indexer servers. The Indexers replicate each other's data so that the system can store multiple copies of all data transiting through Splunk to prevent data loss and promote data search availability.

Heavy Forwarder – The Heavy Forwarder is responsible for collecting and delivering event feeds to Splunk Indexers for processing. It parses and defines data before forwarding it, and can route data based on defined criteria, such as source or event type. It can also index data locally while forwarding the data to another indexer.

Cluster Manager – Manages the overall cluster of components across the Splunk deployment for USA-P-AAP devices. It is responsible for ensuring data replication and search factors are met.

Search Head – Search Head serve as a central resource for searching data across the entire Splunk environment. They handle search management functions, directing search requests to a set of search peers and then merging the results back to the user. Analysts (ISSO, SO, administrators, SOC personnel, etc.) can run or access the same searches, dashboards, knowledge objects, and so on, from any member of the cluster via the Search Heads.

Deployment Server – Acts as a centralized configuration manager for any number of other Splunk instances, called "deployment clients" (e.g., Splunk forwarders or indexers). It is used to deploy configuration updates to all the other Splunk instances in the USA-P-AAP environment.

Cribl – Cribl is a data compression software that is used to enhance Splunk's data ingestion capabilities, helping with log management. Cribl compresses the large volumes of data collected by EOUSA endpoints into a reduced volume data set, helping to ease the load and license usage on Splunk Enterprise.

SOAR – Splunk Security Orchestration, Automation, and Response (SOAR) allows for the automation of manual tasks to address and respond to more alerts in less time. SOAR is designed to integrate and coordinate security tools for automated threat detection and response. It provides workflows and playbooks that the SOC team can leverage to streamline security operations as well as organize security processes and procedures.

More detailed information about SOAR can be found here: https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation.html

UBA – Splunk User Behavior Analytics (UBA) focuses on tracking user behaviors, with devices and applications as the primary entities. UBA aggregates ingested events, storing them in a scalable "analytics" store to reduce raw events. The aggregation granularity and retention period for events is configurable.

UBA profiles normal behavior for each identity and asset, and then looks for unusual behavior patterns across those identities and assets. To help ensure security analysts can focus on critical threats that pose the greatest risk to the organization, once UBA identifies anomalies, it looks for unusual patterns in the captured anomalies for alerting purposes.

More detailed information about UBA can be found here: https://docs.splunk.com/Documentation/UBA/5.3.0/User/UBAContent#:~:text=UBA%20provides%20models%20that%20can,anomaly%20action%20and%20score%20rules

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	40 U.S.C. 1441
Executive Order	Executive Order 14028
Federal regulation	Federal Information Security Modernization Act of 2014, OMB Memorandum M-21-31
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	Office of Management and Budget (OMB) Circular No. A-130; DOJ Order 0904: Cybersecurity Program

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	Some EOUSA systems that send logs to USA-P-AAP are accessible by other federal government personnel and members of the public
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by members of the public who may use their personal email address for access
Personal phone number	X	C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by members of the public who may use their personal email address for access
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			

(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
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			

(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
System admin/audit data:			
- **User ID**	X	A, B, C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by other federal government personnel and members of the public
- **User passwords/codes**	X	A, B, C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by other federal government personnel and members of the public
- **IP address**	X	A, B, C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by other federal government personnel and members of the public
- **Date/time of access**	X	A, B, C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by other federal government personnel and members of the public
- **Queries run**	X	A, B, C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by other federal government personnel and members of the public
- **Contents of files**	X	A, B, C, D	Some EOUSA systems that send logs to USA-P-AAP are accessible by other federal government personnel and members of the public
Other (please list the type of info and describe as completely as possible):			

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		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify):					

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)			

Government sources:
Other (specify):

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
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	Splunk administrators can log into the servers and view all data that has been captured/logged by the system
DOJ Components	X			Sharing data with JMD on a case-by-case basis to support security incident investigations
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

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.

All USA-P-AAP audit logs come from EOUSA information systems. Each of these information systems display the DOJ standard warning banner before granting access to a user. This warning banner notes that the user has no reasonable expectation of privacy regarding any communications transmitted through or data stored on the information system they are accessing, and that at any time the government may monitor, intercept, search and/or seize data transiting or stored on the information system they are using. This system is also covered by DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021), which provides notice to the public regarding this information system.

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.

By agreeing to the displayed warning banner before using an information system, the individual agrees to the conditions that their information will be collected. To opt out of information collection, the individual would have to decide not to use the information system.

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.

This option does not exist within USA-P-AAP. USA-P-AAP is a log collector that ingests data sent from interconnected information systems across EOUSA. Individuals would have to request access or amendment of their data from the information system that they are using that sends system logs to USA-P-AAP. Moreover, the applicable system of records, DOJ-002, Department of Justice Information Technology, Information System,

and Network Activity and Access Records, is exempted from subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1), (e)(4)(G), (H), and (I); and (f) of the Privacy Act of 1974, as amended.

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):** Issued 3/11/2024; Expires 3/12/2027 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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: N/A**
	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:** USA-P-AAP has been categorized as a Moderate system. All applicable, moderate baseline controls are implemented and assessed accordingly. Any controls that are not implemented are tracked for remediation in a POAM.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Security controls are reviewed on a continuous basis, and the system is authorized by the CIO every three (3) years.
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.

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**.
X	**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:** All internal users will complete general information security and privacy training, as well as training specific to the system.

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?

Access controls are implemented to ensure that only authorized users have access to the information collected. Authorized users are only granted the privileges necessary to accomplish their job duties. Individuals with access to the USA-P-AAP web interface to perform audit log searches include USA-P-AAP system administrators and authorized information security specialists (e.g. ISSOs, SOs, etc). Only USA-P-AAP approved system administrators have privileged permissions to the back end of the system to create, edit, modify, and delete information at the application or server level. All user activity is logged within the system and traced back to a specific user. USA-P-AAP devices are not publicly accessible; all devices are only accessible from the DOJ network.

Access to USA-P-AAP is restricted to the DOJ network. Authentication to the end user dashboard is done via USAauth (Okta) single sign-on and PIV card by verified DOJ users. All login actions are audited to ensure that no unauthorized users have been granted access to the system, and all audit logs are reviewed on a weekly basis by the ISSO.

Additionally, all information is automatically encrypted in transit via TLS 1.2 and AES 256. The encryption itself is also tested, based on security controls, during the assessment process and prior to system authorization.

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.

USA-P-AAP logs are retained for a period of seven (7) years. All information collected by the system is disposed of in accordance with DOJ Network Account Records

Management USAP No. 3-13.300.004. 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.

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:

DOJ-002 Department of Justice Information Technology, Information System, and Network Activity and Access Records; https://www.gpo.gov/fdsys/pkg/FR-2017-05-25/pdf/2017-10780.pdf

JMD-026 Security Monitoring and Analytics Service Records; https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-15883_jmd_026_sorn.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.

All EOUSA component systems, including USA-P-AAP, are subject to continuous assessment and authorization processes that ensure that security controls are in place to protect the confidentiality, integrity, and availability of all information and the systems that house that information. For example, access controls based on the principle of least privilege are implemented to ensure that only authorized users have access to the information collected and to ensure that those who have access to the system are only granted the minimum access required based on job duties.

USA-P-AAP users are required to complete mandatory security awareness, privacy, and role-based training on an annual basis. Additionally, all sensitive information is automatically

encrypted in transit by USA-P-AAP, utilizing TLS 1.2 and AES 256. The encryption itself is also tested, based on security controls, during the assessment process and prior to system authorization.

Only system administrators approved by the system owner have privileged permissions within the system to create, edit, modify, and delete information. All user activity is logged within the system and traced back to a specific user, and logs are reviewed on a weekly basis. USA-P-AAP security personnel conduct a privileged user audit on an annual basis to ensure that only active and approved administrator accounts exist within the system. Additionally, USA-P-AAP devices are not publicly accessible; all devices are only accessible from the DOJ network.

All users with access to USA-P-AAP must complete annual Cybersecurity Awareness Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using the IT systems, provides a review of the user's role in protection of these systems, and established guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also sign a Rules of Behavior agreement annually confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training can result in termination of the employee or contractor's access to EOUSA systems, including USA-P-AAP. Participation in the training course is tracked by EOUSA.