Drug Enforcement Administration

Aviation Division (SG)

Privacy Impact Assessment
for the
Aviation Division Office Internet (ADOI)

Issued by:
David J. Mudd, Associate Chief Counsel,
Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: September 30, 2022

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Aviation Division Office Internet (ADOI) is a Hybrid Cloud Environment utilizing Microsoft Azure Government (MAG) with physical servers and workstations located on premises at the DEA Aviation Division (SG). ADOI is the primary information technology communication infrastructure for the Aviation Division's Aviation Operations Center (AOC). ADOI is designed to ensure optimum communications with AOC's internal and external aviation specific applications, and its users and vendors.

The primary applications used on the ADOI domain are Pentagon2000 SQL (P2k), and the SG SharePoint site. The applications are owned by DEA but primarily managed and used by contract personnel. The P2k application is a Microsoft SQL based enterprise resource package focusing on maintaining data records for the maintenance, repair, and overhaul (MRO) operations requirements of DEA's aviation assets; P2k also handles MRO acquisitions, inventory and accounting functions. The software is configured to ensure the AOC's certification as a Certified Aviation Repair Facility is maintained in accordance with the Federal Aviation Administration's (FAA) mandates. Compliance is achieved by documenting and validating the accuracy of maintenance performed on Office of Aviation aircraft as well as adherence to specific business rules regarding parts inventory, work orders, repair, operations, etc. The software has a robust reporting module capable of reporting on information entered into the database including, statistical and trend analysis, cost and maintenance forecasting, and maintenance scope compliance. User access is via a front-end client installed on the users' workstation.

ADOI applications do not interface with each other. The Aviation SharePoint site provides interoperable gap solutions to fulfill any inadequacies or voids. Users are granted email through DEA's Firebird system.

Overall ADOI functions are to facilitate the information sharing and data processing for users of P2k and the internet.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, 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.

The primary purpose of ADOI's data collection efforts is safety of flight. This system and its applications are used to collect all maintenance related data, e.g., forecast maintenance events, record asset utilization, and request and purchase parts. While the activities of ADOI are not law enforcement centric, the entire operation is used to ensure that DEA's Enforcement operations are conducted safely pursuant to the Controlled Substances Act. If information generated by ADOI is used for a law enforcement purpose, that data is stored in Concorde, which is covered under its own Privacy Impact Assessment.

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
X	Statute	21 U.S.C. § 878, Controlled Substances Act
	Executive Order	
X	Federal Regulation	14 CFR Parts 21, 23, 25, 27, 29, 33, 35, 39 43, 45, 47, 65, 91, 133 and 145
	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	Names will/may be collected on employees, contractors, detailees other federal government personnel, members of the public, USPERS and/or Non-USPERs.
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)	X	C, D	For financial accounting and accounts payable processing, vendor TIN numbers will be utilized and collected; this may include USPERs and/or Non-USPERs for
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A, B	Type, model, and tail number will be collected for DEA Aviation aircraft.
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant 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
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			
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	X	A, C, D	Procurement and/or contracting records may be collected on employees, contractors, and detailees, who may be USPERS or Non-USPERS.
Proprietary or business information	X	C, D	Vendors' business names and addresses will be collected for DEA Aviation procurement of parts or supplies; these may be USPERs or Non-USPERs.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			

(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
- **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)**			
System admin/audit data:			
- **User ID**	X	A	System admin/audit user id information will be collected of employees, contractors, and/or detailees.
- **User passwords/codes**	X	A	System admin/audit passwords will be collected of employees, contractors, and/or detailees.
- **IP address**	X	A	System admin/audit IP address information will be collected of employees, contractors, and/or detailees.
- **Date/time of access**	X	A	System admin/audit date/time of access will be collected of employees, contractors, and/or detailees.
- **Queries run**	X	A	System admin/audit for queries run will be collected of employees, contractors, and/or detailees.

(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
- **Content of files accessed/reviewed**	X	A	System admin/audit related information etc. could be collected of employees, contractors, and/or other federal government personnel
- **Contents of files**	X	A	System admin/audit for contents of files will be collected of employees, contractors, and/or detailees.
Other (please list the type of info and describe as completely as possible):	X	C, D	GSA number may be collected on USPERs and Non-USPERs.

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	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
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		X	Direct log-in access for daily update and monitoring of aircraft maintenance requirements. As requested or required, in report or csv. Export file format.
DOJ Components				
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.

ADOI does not release information to the public for open data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of

Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

ADOI's notice to the public is covered under system of records DEA-021, DEA *Aviation Unit Reporting System*, 65 Fed. Reg. 24986, 987 (Apr. 28, 2000) https://www.govinfo.gov/content/pkg/FR-2000-04-28/pdf/00-10687.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.

There are no opportunities for individuals to voluntarily participate in the collection, use or dissemination of information in the system. Information pertaining to individuals is obtained pursuant to FAA mandates for Aviation MRO to include maintenance, acquisitions, inventory, repairs, etc. There is no method for individuals to consent to the use of their information on procurements, invoices, etc.

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.

ADOI is only available to authorized users with permitted access. This allows for approved users to access the information as it pertains to their specific job functions. Individuals may request access to or amendment of their records maintained in ADOI through a FOIA and Privacy Act (FOIAPA) request in accordance with applicable law. A FOIAPA request can be made through the DEA FOIA office.

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):** The most recent ATO was issued June 30 2021 and will expire on Dec. 27, 2024. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A

	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: There are no outstanding POA&Ms.
	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: N/A
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ADOI security evaluation occurs per guidance defined in DOJ's Security Control Assessment Frequency.
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:** All system logs are fed into DEA's Security Information and Event Manager (SIEM), Splunk. Splunk forwarders send log data into the Splunk application. The Splunk application establishes a baseline of activity and alerts when anomalies are detected.
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**. Yes, as a standard operating procedure, all DEA contracts have the necessary, proper and accurate Privacy Act clauses and language.
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 DEA and contract personnel receive Cyber Security Awareness Training (CSAT) on an annual basis and agree to comply with an information technology "rules of behavior" (IT Rules of Behavior).

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?***

AOC enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides by verifying individual access authorizations before granting access to the facility.

ADOI employs the principle of least privilege and enforces role based access control (RBAC), allowing only authorized access to information necessary for users to accomplish their assigned tasks in accordance with their roles. ADOI users consist of privileged and non-privileged users. Privileged users fulfill the role of system administrator and are responsible

for the maintenance and operation of the system, including backing up the system and its recovery. Non-privileged users access ADOI to leverage P2k and the internet.

All data stored, processed, and transmitted within ADOI is encrypted. DEA leverages Splunk to monitor for anomalous or suspect activity. ADOI is protected by boundary protection devices (e.g., firewalls, intrusion prevention systems) at ingress/egress points, and malware protection is deployed throughout the environment.

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.)

The disposition standards for the Federal records in the ADOI system are implemented and followed in accordance with the NARA retention schedule 1180-06 (N1-170-94-1) Aircraft Service Files.

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:

DEA-021, DEA *Aviation Unit Reporting System*, 65 Fed. Reg. 24986,987 (Apr. 28, 2000), https://www.govinfo.gov/content/pkg/FR-2000-04-28/pdf/00-10687.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?

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the DEA's official duties is always a potential threat to privacy. The ADOI system collects and maintains only that information about an individual that is relevant and necessary to

accomplish DEA's mission. ADOI collects and maintains information about an individual that is relevant and necessary regarding aircraft maintenance, repairs, and/or overhaul to include acquisitions, inventory and accounting functions.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the DEA's use of the information in the ADOI system include the risks of unauthorized access to or disclosure of PII. DEA mitigates this risk through multiple controls. Users may only use DEA's secure Firebird system for email. Only authorized individuals are given access to this information. Each user annually is required to review and agree to the DEA IT Rules of Behavior as part of the mandated online CSAT Training, which includes rules on the proper handling of DEA information. The limited distribution of the information from the applications, continual monitoring of access to the applications, and the observance of the IT Rules of Behavior, also limit privacy risks. Outside of DEA, Federal Government users must also comply with computer security requirements, participate in annual security training, and acknowledge updated rules of behavior.

In addition, the method of generating and maintaining User IDs and passwords is one of numerous safeguards DEA uses to protect PII. To maintain system security, the user accounts becomes inactive after a specified number of failed logon attempts or after an extended period of time of no account activity.

DEA manages access by utilizing ADOI through permission-based role assignments and only for individuals assigned to the Aviation Facility.

Immediate notification is relayed to AOC for revocation of access when a user departs DEA. All DEA personnel and contractors have been cleared to work on the system and comply with the security policies and procedures established by DEA.

c. Potential Threats Related to Dissemination

Security measures that are in place to safeguard sharing of information include: IT monitoring tools; firewalls; intrusion detection and data loss prevention mechanisms; and audit logs. Consistent with FISMA and NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), or Secure Sockets Layer (SSL). The database is stored on a fully secured server created and administered in compliance with the Federal Information Security Modernization Act of 2014 and Office of Management and Budget (OMB) guidance.