Drug Enforcement Administration

Privacy Impact Assessment
for the
Aviation Maximo Maintenance Repair and Overhaul (MRO)

Issued by:
James Robert Bryden
DEA Senior Component Official for Privacy

Approved by: Andrew J. McFarland
Senior Counsel
U.S. Department of Justice

Date approved: July 28, 2025

(July 2023 DOJ PIA Template)

Section 1: Executive Summary

The Aviation Maximo Maintenance Repair and Overhaul (MRO) system is an application suite offered as Software as a Service (SaaS) managed by IBM Corporation Enterprise Asset Management hosted in the U.S. Government Cloud. Aviation Maximo MRO system allows the Drug Enforcement Administration (DEA) Aviation Division to perform three key functions:

- Scheduling and managing aircraft maintenance through evaluation of available labor skills using a specialized application.
- Tracking and recording personnel and pilot training certifications and qualifications for approved work assignments.
- Managing inventory and tooling for performance of maintenance.

The Aviation Maximo MRO system maintains data records for the maintenance, repair, and overhaul requirements of DEA's aviation assets. The Aviation Maximo MRO system also allows the DEA Aviation Division to integrate fixed-wing and rotary aircraft asset lifecycle management in one repository, including maintaining a record of aircraft operational data. The Aviation Division uses the Aviation Maximo MRO system to plan and graphically schedule resources for aviation maintenance tasks.

The Aviation Maximo MRO system also handles acquisitions, inventory and accounting functions. Utilizing the Aviation Maximo MRO system ensures that the DEA Aviation Office is operating in compliance with Federal Aviation Administration's (FAA) mandates and regulations. Compliance is achieved by documenting and validating the accuracy of maintenance performed on all DEA's aircraft to include adherence to specific business rules regarding parts, inventory, work orders, repair, operations, etc.

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.

Aviation Division users (employees, contractors, and Task Force Officers (TFOs)[1]) access the Aviation Maximo MRO system SaaS in the U.S. Federal Cloud through the DEA Firebird network, utilizing Firebird-connected workstations or Firebird-managed mobile devices.[2] The Aviation Maximo MRO system permits the Aviation Division to keep aviation related personnel records, track inventory, and perform the upkeep of aviation assets through manual entries performed within the

[1] Task Force Officers are state, local, or tribal law enforcement officers who are deputized and co-located with DEA law enforcement units.

[2] Firebird is covered by separate privacy compliance documentation

Aviation Maximo MRO system application. The Aviation Maximo MRO system provides the same functionality as its predecessor, the Aviation Division Office Internet (ADOI) Pentagon 2000 Structured Query Language (SQL) (P2k) application, which had maintained data records for the maintenance, repair and overhaul operations requirements of DEA's aviation assets. However, the Aviation Maximo MRO system is operated and maintained within the IBM Maximo and IBM TRIRIGA[3] application suite on the U.S. Federal Cloud (Maximo/TRIRIGA SAAS). DEA Aviation Division employees and contractors will access Aviation Maximo MRO system using Firebird workstations and mobile devices. Authentication is accomplished using DEA OKTA for Single Sign On (SSO).[4]

Access to Aviation Maximo MRO system is limited to the DEA Aviation Division government personnel, contractors, and TFOs only. Only DEA Aviation Division government personnel and contractors are assigned as maintainers and/or pilots. TFOs may perform only enforcement operations.

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. § 11314 (Authority to Acquire and Manage Information Technology) 44 U.S.C. § 3101 (Records management by agency heads; general duties) 21 U.S.C. § 801 et seq, Controlled Substances Act
Executive Order	
Federal Regulation	14 CFR Parts 21, 23, 25, 27, 29, 33, 35, 39, 43, 45, 47, 65, 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.

[3] IBM's TRIRIGA is an integrated workplace management system (IWMS) that centralizes facility management processes, among other functions. https://www.ibm.com/docs/en/tririga.
[4] OKTA is a third party service that manages and secures user authentication in applications, offering a single-sign-on service that allows users to log into a variety of systems using a single centralized process.

(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
Name –	X	A, B, C and D	First name, Last Name and middle initials will be collected on employees, contractors and TFOs, including foreign and domestic vendors used by DEA's Total Aviation Support Services contractor, who may be 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 truncated) –			
Tax Identification Number (TIN) –	X	A, C and D	Tax ID Numbers for vendor company will be utilized and collected of DEA contractors, and members of the public (USPERs and/or Non-USPERs).
Driver's license-	X	A, C and D	Drivers Licenses, FAA Pilot and Mechanic certificate numbers of DEA and Contractor personnel, including foreign and domestic vendors used by DEA's Total Aviation Support Services contractor, will be maintained in the system.
Alien registration number –			
Passport number –			
Mother's maiden name –			
Vehicle identifiers –	X	A	Vehicle identifiers for aircraft will be collected including type, model, and tail number of DEA Aviation Assets.
Personal mailing address –			
Personal e-mail address –			
Personal phone number –			
Medical records number –			

(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
Medical notes or other medical or health information –	X	A	Medical Certification for Pilots (DEA employees and contractors) is maintained; Maintainers must have medical certificates for their commercial driver's licenses and Pilots must maintain their medical certificates for their FAA Pilot licenses.
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			
Certificates	X	A, B, C and D	Pilot and Maintainer Certificate numbers of DEA and Contractor personnel, including foreign and domestic vendors used by DEA's Total Aviation Support Services contractor will be maintained in the system.
Legal documents			
Device identifiers, e.g., mobile devices –	X	A	Electronic device identifiers will/may be collected on employees and contractors that are using 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-			

(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
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, B, C and D	Procurement and/or contract records may be collected identifying employees, contractors, and TFOs; also including foreign and domestic vendors used by DEA's Total Aviation Support Services contractor (USPERS or Non-USPERS).
Proprietary or business information	X	A and B	Business contact information will be collected on employees, contractors, TFOs.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
Photographs or photographic identifiers –			
Video containing biometric data –			
- **Fingerprint**			
- **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:	X*	A	System admin/audit data will/may be collected on employees, contractors, and TFOs.*
User ID	X	A	Same as above
- **User passwords/codes**	X	A	Same as above
- **IP address**	X	A	Same as above
- **Date/time of access**	X	A	Same as above
- **Queries run**	X	A	Same as above
- **Contents of files**	X	A	Same as above

(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
Other (please list the type of info and describe as completely as possible):			

- **NOTE:** System Admin/Audit Data: Auditing information as identified above is collected as part of the process of documenting activity within the software. Audit logs record the occurrence of an event, the time at which it occurred, the responsible user or service and the impacted entity.

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		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)			
Other (specify): The primary source of information will be manual input by personnel within the Component. In some areas of operation, there are State, Local, Tribal and Other DOJ Component personnel who may provide manual input to the system. At this time there are no external systems providing input.					

Non-government sources:					
Members of the public		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	System admin/Auditing data may be used/shared to troubleshoot issues with applications. As requested or required, updates of aircraft maintenance may be exported in csv file format
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public	X			Select information would only be shared where required by law or court order.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			System admin/Auditing data information may be required by law enforcement from other organizations for investigations regarding cybercrimes or by courts in civil litigation.
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.

Aviation Maximo MRO system does not release data 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.

Aviation Maximo MRO system'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.

Authentication to the Aviation Maximo MRO system includes providing the below generalized notice. All users are presented with the following banner notice prior to logging onto the Aviation Maximo MRO system. This banner explains to the user their rights as it pertains to using Aviation Maximo MRO system. It should be noted that all users access the Aviation Maximo MRO system through Firebird and complete authentication through OKTA which also displays the DOJ approved banner. The banner reads:

> *You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:*
>
> *The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, Communications Security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.*
>
> *At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS is not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.*
>
> *Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.*

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 maintenance, repair and overhaul 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.

The audit data collected is for system administrative/troubleshooting purposes. If a user requires auditing information, the request should go through the proper channels to include utilizing the helpdesk.

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.

Aviation Maximo MRO system is only available to authorized users with permitted access. This allows 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 Aviation Maximo MRO system 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):** 4/14/2025 expires 07/31/2025 **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:**
	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 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 FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Aviation Maximo MRO system was assigned the security category of Moderate as defined in FIPS-199 based on the aggregation of the information of several different and seemingly

	innocuous types of information (e.g., , first/last name, driver's license, tax identification numbers, FAA certificate numbers) together reveal sensitive information.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, updates to the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle. DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorization by the DEA Authorizing Official. Significant changes that affect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the Senior Component Official for Privacy prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
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:** In accordance with, and agreed upon by FedRAMP, auditing on Aviation Maximo MRO system is the responsibility of the vendor. All of the Aviation Maximo MRO system components generate logs that may be used for auditing purposes. By reviewing the audit logs, system administrators can track user activity, and the security teams (Incident Response Teams) can investigate breaches and ensure compliance with regulatory requirements such as National Institute for Standards and Technology (NIST) 800-53 Rev 5.[5] Aviation Maximo MRO system audit logs capture the following types of information: • Event name as identified in the system. • Description of the event. • Event timestamp • Actor or service that created, edited, or deleted the event (user ID or Application Programming Interface ID) • Application, device, system, or object that was impacted (IP address, device ID, etc.) • Source from where the actor or service originated (country, host name, IP address, device ID, etc.)

[5] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

	Further, DEA Cybersecurity Operations, Response and Engineering Unit (TCVV) is responsible for reviewing and analyzing the Firebird information system audit records on a daily and continuous basis for indications of inappropriate or unusual activity in accordance with DEA Incident Response Plan. DEA TCVV monitors Firebird components using the Splunk event correlation tool[6] to identify and report findings to the ISSO for further investigations upon detection of suspicious activities. Any findings are reported to DOJ Security Operations Center using the Justice Management Division Remedy ticketing system.
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, all contracts have the necessary, proper, and accurate privacy and security-related clauses (i.e., DOJ Clause 02, *Contractor Privacy Requirements*; and DOJ Clause 05, *Security of Information and Information System*) and language required listed in each contract awarded within DEA. .
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:** Required training is distributed and tracked via the DEA Learning Management System (DEALS). This training includes general mandatory annual training for information systems like rules of behavior and cybersecurity awareness training that are applicable to all DEA component personnel, and DEA is implementing annual refresher privacy training in 2025.

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?

Administrative privacy and security controls:

Aviation Maximo MRO system employs the principle of least privilege and enforces role-based access control allowing only authorized access to information necessary for users to accomplish their assigned tasks in accordance with their roles. Users consist of privileged and non-privileged users. Privileged users have been granted access via the Aviation Maximo MRO system application once approval has been granted by the DEA Aviation Division. Non-privileged users access Aviation Maximo MRO system once authenticated through Firebird Microsoft Active Directory and DEA OKTA.

[6] Splunk is covered by separate privacy documentation here: https://www.justice.gov/d9/2023-01/doj_laas_pia_final_for_publication_1.pdf.

The Aviation Maximo MRO system is an application suite offered as SaaS managed by IBM Corporation Enterprise Asset Management hosted in the U.S. Government Cloud. The security safeguards implemented for the IBM Maximo and TRIRIGA on Cloud for U.S. Federal system meet the policy and control requirements set forth in this System Security Plan. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. Aviation Maximo MRO system has been evaluated at a System Sensitivity Level: Moderate

Technical privacy and security controls

The Aviation Maximo MRO system ensures all data stored, processed, and transmitted is encrypted. DEA leverages Splunk to monitor for anomalous or suspect activity. The DEA network is protected by boundary protection devices (e.g., firewalls, intrusion prevention systems) at ingress/egress points, and malware protection is deployed throughout the environment.

The Aviation Maximo MRO system is an application suite offered as SaaS managed by IBM Corporation Enterprise Asset Management hosted in the U.S. Government Cloud. The security safeguards implemented for the IBM Maximo and TRIRIGA on Cloud for U.S. Federal system meet the policy and control requirements set forth in this System Security Plan. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. The Aviation Maximo MRO system has been evaluated, and received FedRAMP authorization to operate, at a System Sensitivity Level: Moderate

Physical privacy and security controls:

Physical access to the Aviation Maximo MRO system servers is the responsibility of the vendor as Aviation Maximo MRO system is a “Software as a Service” instantiation. Physical protection is offered to the workstations as they are housed at the Aviation Operations Center that includes a 12-acre plot that is completely surrounded by concrete walls and utilizes numerous safeguards to include guards who monitor the facility and cameras which are monitored all the time. In addition, the facilities supply electrical and HVAC systems. Entry includes utilizing a Personal Identity Verification (PIV) Card which is scanned for entry and also controls all access points.

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 Aviation Maximo MRO system are implemented and followed in accordance with the DEA Records Information Systems (DEARIS) Handbook, Subsection 1180, Aircraft Maintenance 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

Privacy Risk: Individuals may be unaware their PII is being collected and cannot meaningfully consent to the collection of their PII by Aviation Maximo MRO system.

Mitigation: This risk is mitigated by the use of the mandatory banner at login. Individuals are presented with the same banner (which is described in detail above in Section 5.1) indicating that their PII is being collected. Note: collection of the PII within the systems using Aviation Maximo MRO system are subject to their own notice requirements, if applicable.

Privacy Risk: DEA may collect and maintain more personal information than necessary to accomplish the DEA's official duties.

Mitigation: This risk is mitigated as the Aviation Maximo MRO system only collects and maintains information about individuals that is relevant and necessary to accomplish the DEA's mission. This is accomplished as data entry in the system is only possible through manual processes. The system utilizes structured and limited data fields that are clearly labeled as to their purpose to ensure that personnel are only entering t information about an individual that is relevant and necessary for aircraft maintenance, repairs and/or overhaul to include acquisitions, inventory and accounting functions.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: Potential susceptibility of system information either at rest or in transmission to compromise from an "Insider Threat" or technological/cyber breach (e.g., Hacking) resulting in a breach.

Mitigation: This risk is mitigated. The Aviation Maximo MRO system has implemented a Data at Rest and Data in Transit encryption solution which has been validated utilizing security guides. Further, there are numerous security tools deployed at critical locations within DEA as well as within the Aviation Maximo MRO system environment to ensure any compromise is identified and that the DEA Enterprise Incident Response Plan has established processes to follow in the case of compromise. 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., Point to Point IPSEC Tunnel, Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), or Secure Sockets Layer (SSL). See also the measures described above in Sections 6.1 and 6.2.

Privacy Risk: Authorized DEA personnel may mishandle or fail to safeguard PII.

Mitigation: This risk is partially mitigated. The Aviation Maximo MRO system utilizes numerous security tools to ensure that the system components are securely configured and managed in accordance with policy. However, there remains some possibility DEA personnel may not handle PII data in accordance with policy. Therefore, users receive annual Computer Security Awareness Training (CSAT) as well as annual refresher Privacy Act trainings, and are expected to follow DEA IT Rules of Behavior that defines PII requirements to the users of DEA's IT systems. All users are required to review and provide signature or electronic verification acknowledging understanding of these rules.

Privacy Risk: The administrative control environment established for the system may not sufficiently define the roles and responsibilities of DEA personnel with respect to handling and protecting PII to ensure only authorized access.

Mitigation: This risk is mitigated. The administrative control environment described in section 6.2 assures that only authorized individuals are given access to this 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.

TFOs from other Federal Government agencies must also comply with computer security requirements, participate in annual security training, and acknowledge updated rules of behavior. Further, as part of completing the annual core control review as defined by DOJ and the quarterly review of any outstanding POAMs as defined by DEA, the roles and responsibilities as defined for both users and managers are validated annually to include not only applicability but to also ensure compliance.

Further, the documentation setting forth roles and responsibilities is reviewed/reassessed annually. (See Section 6.1, explanation box re: monitoring, or Section 6.2) Also, 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.

Privacy Risk: PII information may be accessed and altered for potentially impermissible purposes, thereby affecting the accuracy and reliability of the information.

Mitigation: This risk is mitigated. The Aviation Maximo MRO system does not ingest data from other sources. Therefore, if data is altered, the security tools would alarm DEA TCVV. (See Section 6.1, explanation box re: monitoring, or Section 6.2) Use of Aviation Maximo MRO is limited to authorized Aviation users. Users are vetted through DEA background check, and the user's supervisor must confirm access before being granted access with a limited role-based permission assigned within the application. Further, users are required to review and provide signature or electronic verification acknowledging understanding the rules identified in the DEA IT Rules of Behavior.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: DEA personnel may share or disclose PII Information to an inappropriate party, for an improper use, or in a manner inconsistent with the relevant routine uses and DEA/DOJ policy.

Mitigation: This risk is mitigated because users of Aviation Maximo MRO system are required to review and provide signature or electronic verification acknowledging understanding the rules identified in the DEA IT Rules of Behavior. All users of Firebird workstations are required to review and provide signature or electronic verification acknowledging understanding the rules identified in the DEA IT Rules of Behavior including limitations on dissemination of PII. DEA also implemented annual role-based privacy training that addresses the safeguarding and proper dissemination of PII. Further DEA personnel are continuously made aware of privacy expectations through the use of the mandatory banner at login.

Privacy Risk: DEA's controls may be insufficient to prevent unauthorized individuals within DEA or DOJ from accessing the system's PII without having a need to know.

Mitigation: This risk is mitigated. This mitigation occurs through multiple security tools working alongside user access and training help mitigate this risk. (See Section 6.1 and Section 6.2). In particular, Qualys, along with other security tools, continues to monitor access to data that is available for use by Aviation Maximo MRO system.

The method of generating and maintaining User IDs and passwords is one of numerous safeguards DEA uses to protect PII. To maintain system security, Aviation Maximo MRO system utilizes Firebird authentication to include Group Policies that ensure the following:

- User accounts that become inactive after a specified number of failed logon attempts are locked;
- User accounts that become inactive after an extended period of time are locked; and
- All user accounts are managed as part of Firebird Account Management Processes.

Further, only authorized individuals assigned to the Aviation Division are given access to the system. DEA manages access to Aviation Maximo MRO system through permission-based role assignments. Additionally, DEA system users are permitted only the use of DEA's secure Firebird system for email communication, which is regularly monitored for PII spills outside DEA.

Lastly, all DEA personnel and contractors are required to annually review the security policies and procedures established by DEA for handling PII. Each user is required to review and agree to the DEA IT Rules of Behavior as part of the annually mandated online Cybersecurity Awareness Training (CSAT) Training, which includes rules on the proper handling of DEA information. Outside of DEA, Federal Government users must also comply with computer security requirements, participate in annual security training, and acknowledge updated rules of behavior. DEA also implemented annual role-based privacy training for all DEA personnel (including contractors) that addresses the safeguarding and proper dissemination of PII.