Drug Enforcement Administration

Privacy Impact Assessment
for the
Account Management System

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

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: August 21, 2024

(May 2022 DOJ PIA Template)

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 Account Management System (AMS) is a web-based application that is used to assist in the lifecycle management of user accounts across multiple systems within the Drug Enforcement Administration (DEA). AMS is a Major Application on the DEA Firebird General Support System. This interactive portal enables users to track the status of their accounts in multiple systems. The portal also provides supervisors and managers with a means to track and manage account access and renewal requests for subordinates. Additionally, AMS contains functionality for security analysts to monitor for accounts that are inactive, dormant, rogue, or granted access beyond those required for assigned roles and duties.

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 Account Management System (AMS), formerly known as the Validation, Integrity, Penetration Response (VIPR) Portal, provides automated account management solutions for the Drug Enforcement Administration (DEA) workforce by providing supervisors with the ability to manage information technology accounts and accesses for DEA system users. Individuals identified within AMS include all DEA employees, contractors, Task Force Officers, and any other Federal, State, or local law enforcement officer granted access to the Firebird system. AMS includes an interactive portal for system administration of personnel enabling the tracking of their account management requests as submitted and approved by supervisors and managers. The AMS system also provides Cybersecurity Operations, Response, & Engineering Unit personnel with greater security oversight of account management activities within DEA. Through the AMS system, monitoring of employees' activities is conducted to recertify, enable, disable, or remove accounts no longer required, and identify dormant accounts, rogue accounts, unauthorized accesses, and situations where employees have been granted additional accesses beyond those that are required to perform their job.

The AMS system is a collection of custom-developed AMS modules: Account Management, Account Renewal, User Information, etc. that support the security oversight, verification, and validation of account management activities performed on DEA's classified and unclassified information technology systems. The AMS system itself, however, does not contain any classified national security information. The current AMS system addresses five critical account management oversight and operational responsibilities:

1) enables supervisors to promptly request the removal, disabling, or re-enabling of accounts or accesses for employees who separated or are on extended leave;

2) provides supervisors with an automated solution to review and renew their employees' accounts and accesses to information technology systems annually;
3) provides system administration personnel with a tool to monitor and track account management requests;
4) identifies and flags inactive accounts and creates automated requests to have them disabled or removed, and
5) consolidates information technology account information from multiple sources into a single authoritative identity data store.

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	Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551, et seq. 28 U.S.C. § 534 40 U.S.C. § 11331 44 U.S.C. § 3101
X	Executive Order	Homeland Security Presidential Directive 12 (HSPD-12)
X	Federal Regulation	28 C.F.R. §§ 0.100-104
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	Office of Management and Budget, Circular A-130, "Managing Information as a Strategic Resource; Federal Information Processing Standards (FIPS) 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (Aug. 2013). DOJ Order 0904 – Cybersecurity Program DOJ Order. DOJ Order 2740.1A – Use and Monitoring of DOJ Computers and Computer Systems.

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 and B	Name of DEA Component, Contractors, and Detailees, and Other Federal Government Personnel
Date of birth or age	X	A	Date of birth only for DEA employees...
Place of birth			
Gender	X	A	Gender for only DEA employees.
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A and B	Social Security Numbers (SSN) are stored for DEA/Component Employees, Contractors, Detailees, and Other Federal Government Personnel
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			
Personal phone number			
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	X	A	Job Title, Job Position, Employee Type, Entrance on Duty and Employment Separation Date of DOJ/Component Employees, Contractors, and 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
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			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A and B	Duty Location, Company/Organization, of DEA IT account users of DOJ/Component, Contractors, Detailees, and Other Federal Government Personnel
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			

(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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	User ID for DEA/Component Employees, Contractors, Detailees, and Other Federal Government Personnel
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other types (please list all other types of identifying information collected and describe as completely as possible):	X	A	Information about Sensitive Compartmented Information (SCI) accesses, such as SCI levels, read on dates, and debrief dates; and Request-based information such as type of request, approvals, statuses and workflow data of DEA/Component Employees, Contractors, and Detailees. This system does not contain classified national security information.

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		Other Federal entities	X
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other			

Government sources:					
		documented arrangement related to the transfer)			
Other (specify): National Finance Center					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): Information on themselves.					

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	Information is only accessible to those with a need to know in the performance of duties associated with user account management.
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.

Not applicable. Information will not be released 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.

Notification for those entering PII into AMS has been implemented through a Privacy Act Notice prominently displayed in a popup window for new users and available to all other users for their review as of July 1, 2024. Further, general notice is provided by:

- DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 Fed. Reg. 37188 (Jul. 14, 2021).
- DOJ-006, "Personnel Investigation and Security Clearance Records for the Department of Justice," 67 Fed. Reg. 59864 (Sep. 24, 2002)(full text); 69 Fed. Reg. 65224 (Nov. 10, 2004); 82 Fed. Reg. 24147 (May 25, 2017)(amendments).
- DOJ-020, "DOJ Identity, Credential, and Access Service Records System," 84 Fed. Reg. 60110 (Nov. 7, 2019).

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.

For a new account tracked by AMS, users have the opportunity to enter, correct, or validate their Social Security Number (SSN) and other identifying information.

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 are provided an opportunity when their account is established to enter or correct their SSN and other identifying information. Upon subsequent entry into the system and validation of their SSN, users do not have access to modify their own personally identifiable information (PII). A user must contact the AMS help desk to request PII changes.

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):** June 15, 2020, and expires on January 31, 2024 (An extension to the expiration date has been requested for July 31, 2024, was approved by the DEA CIO.) **If an ATO has not been completed, but is underway, provide status or expected completion date:** Not applicable.
X	**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:** Existing POA&M are associated with technical controls for privacy verification functions, and configuration management associated with the managing PII. Details are contained within the JCAM under POAM IDs: 46558, 47078, and 48458.
	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:** AMS is categorized as a High impact system due to the criticality of the security function it provides and the sensitivity of the data it contains.
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, update of 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 reauthorizations by the DEA Authorizing Official. Significant changes that effect 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, or a duly authorized official, 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:** The application audit logs are reviewed daily as part of the Cybersecurity Operations, Response and Engineering Unit (TCVV) review process. The Operations & Response team reviews all logs forwarded from DEA systems for suspicious behavior and notifies the system owner/security points of contact of any alerts. Additionally, the program management office performs periodic reviews to ensure user and system behavior comply with all applicable DOJ, DEA, and federal guidelines, policies, and laws.
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 contracts have the necessary, proper, and accurate Privacy Act clauses 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:** Department privacy training sufficiently covers information types and concerns applicable to AMS operations. No additional training is required for AMS users or operations personnel.

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?

AMS is a Major Application on the DEA Firebird network and is physically housed at the Sterling Park Technology Center (SPTC), a gated facility with no public access that includes an onsite guard force and 24/7 physical intrusion monitoring. Only those authorized to work in the server rooms at SPTC are granted access to those areas.

Technical controls include extensive use of logical access controls on AMS files and services to prevent unauthorized access to server resources and personally identifiable information. Hard drive encryption is utilized to protect data at rest and all AMS data transiting the network

is also encrypted. As an additional layer of security, the database fields containing SSN are further encrypted to exclude access to Firebird administrators without a need to know for the PII contained within AMS.

Administrative measures involve limiting access to PII through separation of duties and least privilege. Specifically, access to the SSN is tightly controlled through system roles. After a user initially validates their SSN only the last four digits are subsequently displayed. Direct supervisors can only view the last four digits of a subordinate's SSN. Likewise, AMS administrators can only view the last four digits of the SSN through the web interface as well.

Database columns with PII data are encrypted to prevent access by those with administrative access to the operating system who have also not been granted role-based access to the system. Furthermore, successful access to PII data for any query are also audited. Records of audit logs are reviewed at DEA security operations level as well as by the Information System Security Officer.

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.)

Some user account actions become associated with the records of other users, such as when a supervisor approves a subordinate request for access or change. In cases like this, the PII of these individuals is retained for at least three years after both have departed DEA. PII is removed three years after an individual departs DEA and there are no associations with active accounts in the system. There are 8 applications accounts and 6 network accounts that may be applied for on AMS.

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," 86 Fed. Reg. 37188 (Jul. 14, 2021).

DOJ-020, "DOJ Identity, Credential, and Access Service Records System," 84 Fed. Reg. 60110 (Nov. 7, 2019).

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?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

a. Potential Threats Related to The Collection of the Information.

Privacy Risk: Over-collecting and maintaining more personal information than necessary to accomplish DEA's official duties and its mission.

Mitigation: This risk is mitigated. AMS collects only user account attributes such as full name, network & application accounts, account status, supervisor name and position, location, Social Security Number, employee type, position, company, department, telephone number, and employment start/separation dates and any classification authorizations. All data elements collected are necessary for AMS to function in its role.

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

Mitigation: This risk is mitigated. Within the User Information tab on of an individual's personal AMS page the last four digits of their SSN is observable. This same page is reviewed by users during the annual review of their access. Additionally, a Privacy Act notice will be displayed as well to mitigate risk.

Privacy Risk: Individuals may be unaware of DEA processes to access, amend and dispute their PII when collected for non-criminal investigation purposes.

Mitigation: This risk is mitigated. Access to these records is permitted under the Privacy Act and is also outlined in 28 CFR 16 Subpart D. Specifically, all requests for access to these records must be in writing and should be addressed to DEA's Freedom of Information and Privacy Act Unit (CCAR). The request should include a general description of the records sought and must include the requester's full name, current address, date of birth, and place of birth. The request must be signed, dated and either notarized or submitted under penalty of perjury (i.e., DOJ-361 form). Additionally, users can update their profiles in AMS upon log on to correct elements such as their SSN, if that is inaccurate.

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

Privacy Risk: Potential for use of PII in a manner incompatible/inconsistent with the intended uses of or specified purposes for collection of the information.

Mitigation: This risk is partly mitigated. Although all DEA personnel are granted access to AMS by virtue of having a Firebird account and are assigned an AMS default account role, this role only allows them to view their own account information and non-supervisory

personnel cannot see another user's information. Limitation of what information users can access is a type of role-based access control designed to protect sensitive PII of others from misuse. On the other hand, DEA supervisors do have access to their subordinate's information, including the last four of the subordinate SSN. Supervisors can subsequently request from the AMS Helpdesk to obtain full access to a subordinate's SSN which may be needed for verification of individual user being approved. In addition, a handful of AMS administrators also have access to a user's SSN, which is required for verification in conjunction with access requests for systems that process National Security Information.

Privacy Risk: Potential for a system breach by physical intrusion or technical exploitation of the data at rest or in transit.

Mitigation: This risk is mitigated. AMS data at rest is protected with hard-drive encryption that precludes access by physical intrusion and removal of the hardware. Furthermore, database encryption of the SSN field in the AMS database further prevents logical access by those that are not AMS database administrators. All server-to-server and server-to-client access over the network is point to point encrypted by the operating system itself or through Transport Layer Security for web traffic. AMS traffic is further contained with the DEA Firebird system which is bulk encrypted when it exits a DEA facility. All Firebird users are authenticated with a Personal Identity Verification (PIV) card before they can access AMS. In addition, AMS user activity is logged within AMS and regularly reviewed for anomalous activity.

Privacy Risk: Data may be retained longer than necessary, which may reduce the relevance and timeliness of the data.

Mitigation: This risk is mitigated. The PII is only retained as long as it is necessary to match an account with the individual. PII is removed three years after an individual departs DEA and their record of activity is no longer associated with active accounts in the system.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: Potential for DEA personnel to access the information without no need to know or disclose PII to an inappropriate party or for an improper purpose.

Mitigation: This risk is mitigated. Security measures in place to safeguard sharing of information include: IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and system audit logs. In addition, DEA has established minimum auditable events based on DOJ IT security requirements. The information system produces audit records, at a minimum that establish what type of event occurred, when and where it occurred, the source of the event, outcome of the event, and the identity of any user or subject associated with the event. Given that AMS is protected from external access through layers of DOJ and DEA firewalls as well as multifactor authentication, the risk of compromise to PII within the system by malicious insider or malware is lessened. AMS does not transmit PII to other internal systems, and other DEA systems cannot access PII housed within it, thereby eliminating the threat of inappropriate unauthorized access. The primary potential threat to privacy arises from an insider threat. Users with access to the PII could accidentally or maliciously disclose the information accessed. Consistent with

FISMA and NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Transport Layer Security (TLS), or other encryption.