

Drug Enforcement Administration



Privacy Impact Assessment for the Authenticated Digital Asset Management System (ADAMS)

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

Approved by: Kameron Cox
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: Sept. 23, 2026

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 Authenticated Digital Asset Management System (ADAMS) software is used to obtain and process developed “friction ridge details” (i.e., fingerprints and palmprints), also known as latent prints,¹ obtained from evidence specimens submitted to Drug Enforcement Administration (DEA) laboratories. ADAMS consists of three fundamental subsystems: (1) input and central acquisition/management/ tracking, (2) processing/enhancing; and (3) output.

During acquisition, digital cameras and flatbed scanners at ADAMS workstations capture friction ridge detail images. Each unaltered image, called an “asset”, is uploaded into ADAMS in its original .tif file format with an original filename corresponding to its associated case file in DEA’s Laboratory Information Management System (LIMS).² Each image is assigned a unique, secure hash signature that can be used to authenticate the integrity of the original file at any time and verify that it has not been compromised or changed. DEA Friction Ridge Examiners (FRE) use Photoshop software in connection with ADAMS software to enhance the developed images for evaluation, comparison, verification, and technical review purposes. Additionally, the system records an audit trail of each time a user accesses or exports an image; automatically records each processing step during the enhancement process; displays and, upon request, prints both the image enhancement history and an audit trail for each image.

FREs use ADAMS software to reproduce digitized images and share information with other FREs at various laboratory locations since printed hard copies of the images and related information are no longer produced and maintained. ADAMS software enables users to send latent print images to the Federal Bureau of Investigation’s (FBI) Universal Latent Workstation (ULW) to search for matching known print images³ in the FBI’s Next Generation Identification (NGI) system.⁴ ADAMS also allows users to request the known prints of previously identified individuals via ULW.

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

¹ Latent prints are fingerprints or palmprints made of sweat and oil transferred to an object from the friction ridges of a finger or palm.

² LIMS is covered by separate privacy compliance documentation.

³ The term “known prints” refers to the fingerprints or palmprints of an individual, associated with a known or claimed identity, and deliberately recorded electronically, by ink, or by another medium.

⁴ NGI replaced FBI’s Automated Fingerprint Identification System (AFIS), but FBI personnel often refer to NGI as AFIS. Both are covered by separate privacy compliance documentation on FBI’s website.

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.

ADAMS maintains the digital images and documentation that are necessary to support an FRE's comparison of a known print against a latent print and their conclusions. ADAMS also documents the preservation of developed latent prints on evidence. These imaged files are maintained for current law enforcement cases and future court proceedings. Specifically, the system records information required to substantiate the authenticity of the latent print images. This includes documentation of all steps taken during the image capturing and enhancement process. This information is needed for technical reviews, court testimony, accreditation inspections, and verification processes.

ADAMS consists of three fundamental subsystems: (1) input and central acquisition/ management/ tracking, (2) processing/enhancing; and (3) output. Important functions of ADAMS include: authenticating the originality of the images that FREs upload into the system from a camera, the camera's removable SD card, or a flatbed scanner; recording an audit trail of each time a user accesses or exports an image; recording (automatically) each processing step during the enhancement process; then displaying and, upon request, printing the enhancement history and audit trail of each image.

During acquisition, FREs may use a digital camera or flatbed scanner with ADAMS software to capture images of developed friction ridge detail on evidence specimens. Latent prints are generally obtained by DEA from evidence gathered pursuant to an authorized investigation. Whereas DEA directly collects known prints of people who appear to be relevant to an investigation or who are applicants for employment. ADAMS also contains developed latent print images from evidence submitted to DEA laboratories by other federal, state, local, and tribal agencies. Each original image, known as an asset, is uploaded into ADAMS unaltered, in its original .tif file format, with the original file name assigned by the device- and attached to a case file. FREs also input into ADAMS information about each image, such as its capture date, who captured it, its exhibit number, evidence specimen number, friction ridge number, and a description of where a latent print is located on an evidence specimen. The asset is assigned a unique, secure hash signature by the system that can be used to authenticate the integrity of the original file at any time and verify that it has not been compromised or changed. The integrity of the asset can be authenticated at any time. The system creates a new hash value from the bits within the asset and compares the new hash value to the original hash value for that asset, which is stored in the repository. If the hash values match, the asset is unaltered. Additionally, the system records an audit trail of each access or export of an image; records (automatically) each processing step during the enhancement process; and displays and, upon request, prints both the enhancement history and audit trail for each image.

FREs use Photoshop software connected to ADAMS to process and enhance the developed images for evaluations, comparisons, verifications, and technical reviews. Photoshop's image processing tools allow FREs to make the friction ridge detail clearly visible in an image. Photoshop saves an enhancement history for each image. Enhancement history displays the steps used, and the settings and parameters for those steps, when the image is processed using Photoshop. This history is transferred to ADAMS when the FRE saves the image to ADAMS.

ADAMS software provides an FRE the ability to reproduce digitized images and share its outputs with other FREs at various laboratory locations. This is necessary because printed hard copies of known

print images and related information are no longer produced and maintained. ADAMS software enables users to send latent print images to ULW for the purpose of searching for matching known prints in NGI. ADAMS also enables users to request known prints of named individuals from NGI. The connection between ADAMS and ULW is provided by the FBI Law Enforcement Enterprise Portal (LEEP)⁵ via an app called AFIS Connect. AFIS Connect prepares the latent print image (i.e. resizes the image, adjust resolution, etc.) for submission to LEEP through a separate interface. LEEP is a secure platform for law enforcement, intelligence groups, and criminal justice entities to access web-based investigative tools, analytical resources, and information sharing networks. FBI approves LEEP access for DEA FREs and DEA law enforcement personnel (but not contractor administrators). Using the connection through LEEP, ADAMS users send latent print images saved from AFIS Connect to ULW for the purpose of searching for matching known prints in NGI. There is an option to register unidentified latent prints to NGI, where they will remain for future comparison searches. If a potential match is returned by NGI, the system will return information contained on a known print card via LEEP. FRE conclusions and any relevant information returned by NGI is recorded on DEA's LIMS. Any known prints used in a comparison resulting in an identification are stored in ADAMS.

ADAMS also allows users to obtain known prints using the ADAMS transaction manager or latent editor functions to send a request for known print cards to ULW via LEEP and AFIS Connect. Known print cards contain a set of known prints of someone whose identity is already known – such as when taken from someone who is arrested or whose prints have been requested to be kept in the FBI database. Known print cards are submitted by law enforcement personnel—generally FBI, State, or local law enforcement agencies.

Occasionally, the submitting agent will send in a set of known prints to the Office of Forensic Sciences that were taken on a known print card in the field for the laboratory to conduct a search for matching prints in NGI, or, if the agents know that an individual has never been arrested, for any comparisons to friction ridge detail that was obtained from evidence submitted into the laboratory.

ADAMS electronically captures the following Personal Identifiable Information (PII) from known print cards submitted from the field to the Office of Forensic Sciences: names, finger/palm prints, addresses, sex, height, weight, eye color, hair color, tattoos, dates of birth, places of birth, social security numbers, and alias names. However, known print cards retrieved from NGI contain only the names, FBI numbers, and finger/palm prints of individuals. ADAMS captures only this limited information from known print cards retrieved from NGI.

Only FREs with a need to know have access to the print images in ADAMS and the conclusions made on the print images documented in LIMS. ADAMS is fully compliant with the NIST FIPS 180-4 Secure Hash Standard (SHS) requirements, and each digital asset is signed with a unique hash value that provides 256 bits of security (SHA-256). Users will have to use their DEA Personal Identity Verification (PIV) cards on their workstations to access the ADAMS webpage, which is only accessible on isolated machines or machines specifically allowed through DEA's access control lists. PIV credentials are used by the Federal Government to control access to federally controlled facilities and information systems. A contracted engineering team, whose members have gone through DEA security clearance procedures, also has administrative access to ADAMS.

⁵ LEEP is covered by separate privacy documentation.

After analysis of the prints in NGI the FRE then creates and submits a laboratory report with their findings, and any returns from NGI, to the submitting DEA case agent via secure encrypted email. DEA agents also use secure encrypted email to forward lab reports and NGI returns to other agencies that submit evidence for latent print analysis. The reports are maintained in LIMS, and not ADAMS. Submitting agents may perform secondary queries of the NGI System to obtain associated criminal history information and additional biometric images. However, this information is not returned within the initial responses to the searches of latent prints via the NGI System and subsequent searches are conducted outside the Office of Forensic Sciences and are not captured in the ADAMS system. If requested by the prosecutor, all latent images on ADAMS that were developed on a given exhibit that was examined for latent images, can be printed or copied to digital media (DVD or CD) and included with disclosures made during the criminal discovery process.

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	The Comprehensive Drug Abuse Prevention and Control Act of 1970 (Controlled Substances Act), 21 U.S.C. § 801 et. seq.; 28 U.S.C. § 534 (Acquisition, preservation, and exchange of identification records and information; appointment of officials); and 44 U.S.C. § 3101 (Records management by agency heads).
Executive Order	
Federal Regulation	21 C.F.R. § 1300, et seq.
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 *Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to “other” any other types of information.*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
<i>Example: Personal email address</i>	<i>X</i>	<i>B, C and D</i>	<i>Email addresses of members of the public (US and non-USPERs)</i>
Name	<i>X</i>	<i>A, B, C and D</i>	Name of DOJ/Component Members of the Public (US and Non-USPERs) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
Date of birth or age	<i>X</i>	<i>A, B, C and D</i>	Date of birth of Members of the Public (US and Non-USPERs) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
Place of birth	<i>X</i>	<i>A, B, C and D</i>	Place of birth of Members of the Public (US and Non-USPERs) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
Sex	<i>X</i>	<i>A, B, C and D</i>	Sex of Members of the Public (US and Non-USPERs) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
Race, ethnicity, or citizenship	<i>X</i>	<i>A, B, C and D</i>	Race, ethnicity or citizenship of Members of the Public (US and Non-USPERs) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	<i>X</i>	<i>A, B, C and D</i>	Full SSN of DOJ/Component Members of the Public (US and Non-USPERs) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.

(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
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C and D	Personal Mailing address Members of the Public (US and Non-USPERs) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
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	X	A, B, C and D	Military status or other information of DOJ/Component Employees. Contractors, and Detailees, Members of the Public (US and Non-USPERs) potentially captured with submissions of Applicant Card FD-258.
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	X	C and D	FBI UCN (Universal Control Number) and SID (State Identification Number) could be collected from members of public (USPERs and non-USPERs)

(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
Juvenile criminal records information	X	C and D	FBI UCN (Universal Control Number) and SID (State Identification Number) could be collected from members of public (USPERs and non-USPERs)
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			
<i>Biometric data:</i>			
- Photographs or photographic identifiers			
- Video containing biometric data			
- Fingerprints	X	A, B, C and D	Fingerprints of Members of the Public (US and Non-USPERs) captured/recorded by system, with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
- Palm prints	X	A, B, C and D	Palm Prints of Members of the Public (US Citizens or USPERs as well as Non-USPERs) Captured/recorded by system, with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
- Iris image			
- Dental profile			
- Voice recording/signatures			

(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
- Scars, marks, tattoos	X	A, B, C and D	Scars and Tattoos of Members of the Public (US Citizens or USPERS as well as Non-USPERS) potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify) - Height - Weight - Eyes - Hair	X	A, B, C and D	Other specific information about individual that could be processed by ADAMS potentially captured with request of known prints from the FBI or with submissions of Criminal Card FD-249; or of DOJ or other Federal personnel from Applicant Card FD-258.
<i>System admin/audit data:</i>			
- User ID	X	A	User IDs of FREs, DEA-cleared system Engineers and contractors, and the program manager
- User passwords/codes	X	A	Passwords for some DEA/Component Employees, Contractors, Detailees, and other Federal Government Personnel. (Admins)
- IP address			
- Date/time of access	X	A	Log Info. on some DEA/Component Employees, Contractors, Detailees, and other Federal Government Personnel. (Admins)
- Queries run			
- Contents of files			

(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): Originating Agency Identifier (ORI) Originating Case Agency (OCA) Transaction Control Number (TCN) FBI Number Identifiers associated with fingerprints input into ADAMS, such as exhibit numbers, evidence specimen numbers, and friction ridge numbers.	X	A, B, C and D	The following information may also be captured by the system: Character number submitted to identify requesting Agency (e.g. DEA, other federal government agencies, or state and local agencies). A field for the requesting agency to use for internal needs. Identifies payment for the processing of fingerprints. Issued when a new entry on arrest is received. --All such information may be captured with the request of known prints from the FBI or with submissions of Criminal Card FD-249, or Applicant Card FD-258.

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		Online
Phone		Email		
Other (specify): With respect to latent prints, ADAMS software does not gather information directly from the individuals when it contains information about them, however, known prints of individuals and from law enforcement agency partners are obtained directly from individuals.				

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): The NGI system described in Section 2.1 is a source of information. Other federal, state, local, and tribal agencies submit evidence to the lab for print analysis. ADAMS may contain known prints and other information gathered by the foreign agencies if such information is submitted by DEA foreign offices participating in bilateral investigations.					

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	ADAMS information is accessed within DEA as needed by authorized users. Reports of findings are sent to submitting DEA personnel.
DOJ Components	X			ADAMS provides the connection to the FBI Universal Latent Workstation (ULW) for image searches and known print requests.
Federal entities	X			A final fingerprint examination report is sent by secure encrypted email to the submitting agency by the DEA case agent acting as the agency's point of contact.
State, local, tribal gov't entities	X			A final fingerprint examination report is sent by secure encrypted email to the submitting agency by the DEA case agent acting as the agency's point of contact.
Public				

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.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			If digital images are requested by defense attorneys and approved by DEA Office of Chief Counsel, the images are sent to the DEA case agent who coordinates with the prosecutor to provide copies of the images to the defendant's legal counsel.
Private sector				
Foreign governments	X			Digital images are sent to DEA case agents working in foreign field offices, who may share them with foreign agency personnel.
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.*

Data within ADAMS is not released for Open Data purposes and is not used for research purposes.

Section 5: Notice, Consent, Access, and Amendment

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

General notice to the public is provided by the following system of records notices:

JUSTICE/DEA-008 Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012), <https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf>.

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).

Notice is also provided to individuals in situations where a physical print impression is taken from a person for pre-employment screening.

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.*

ADAMS does not give notice to individuals when latent prints are acquired as the purpose of the collection is to determine whether the latent print on the evidence can be identified, and the person may not be present or known. Additionally, for those arrested of a crime, obtaining that person's fingerprints is a mandatory part of the arrest processing protocol and is necessary for several reasons, including maintenance of a person's criminal history records. Thus, it is not necessary to obtain consent from arrested persons. However, persons who are voluntarily fingerprinted as part of a job application, like law enforcement applicants, consent to the collection and uses of their fingerprints and other PII.

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.*

The Federal Rules of Criminal Procedure require that a defendant be provided with a copy of the evidence that will be used in a court proceeding against them, as well as items that are material to the defense. The prosecuting attorney will coordinate with the investigating agent to provide a copy of the appropriate information to the defendant's legal counsel. This process is known as discovery.

The process for requesting access to or amendment of information within ADAMS is found at 28 C.F.R. §§ 16.40-16.49. DEA's response to any request for access or amendment will depend upon the facts pertaining to the request. Non-user related information in ADAMS is retained in DEA's Investigative Reporting and Filing System (and other listed systems of records), which has been exempted from access and amendment requirements of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2) (see 28 C.F.R. §16.98).

Information in ADAMS is also excluded from production under the Freedom of Information Act (FOIA) because it is compiled for investigative law enforcement purposes (see 5 U.S.C. §552(b)(7)). Where compliance would not appear to interfere with or adversely affect the law enforcement or counterterrorism purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the DEA in its sole discretion.

User-related information in ADAMS is subject to the same Privacy Act access and amendment regulations cited above.

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): ADAMS was granted an “Ongoing Authorization” ATO on Feb. 8, 2024. 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: No current Privacy POA&M.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information, and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: ADAMS maintains advanced digital imaging evidence. Under NIST SP800-60 Volume II Revision 1, this information properly falls under D.17.3 Litigation and Judicial Activities – Legal Investigation, with a provisional confidentiality impact level for this type of information being MODERATE. If a loss of confidentiality, integrity, or, availability regarding latent print information were to occur, the worst case scenario would be that individuals may have their prints disclosed to third parties (identified by case or lab numbers) and/or the DEA itself may suffer the loss of digital fingerprint evidence of latent prints which could lead to investigation obstruction or compromise. With respect to known prints, if a loss of confidentiality, integrity, or, availability of known prints were to occur, the worst case scenario would be that individuals may suffer exposure of their identities as well as their prints, potentially a linking individuals as DEA personnel or applicants or as individuals associated with DEA investigations where matches to FBI LEEP results were made, which could result in public embarrassment or in extreme circumstances lead to harassment or a potential for coercion.

	There are no special factors and no mitigating/aggravating circumstances listed that could result in higher or lower impact level.
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 and updates the system security and 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. Changes that may significantly affect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are required to be 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. The system owner is responsible for leading system and user compliance with relevant guidelines, policies, and laws. The Information System Security Officer (ISSO) for ADAMS is responsible for validating that users comply with said governance while TCVV enforces actions based upon an infraction (cybersecurity incidents, policy violations). TCVV performs validation for compliance with governance standards during scheduled risk assessments (ATO renewal or continuous monitoring audit) or remediation efforts against the system during a cybersecurity investigation.
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. All contracts have the necessary, proper, and accurate privacy and security-related clauses (i.e., DOJ Clause 02, <i>Contractor Privacy Requirements</i>; and DOJ Clause 05, <i>Security of Information and Information Systems</i>) 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:

Training specific to this system is conducted by the Friction Ridge training officer on site.

All other DEA-required trainings are distributed and tracked via the DOJ Learning Management System DEALS. This training includes general mandatory annual trainings for information systems, such as rules of behavior and Cyber Security awareness training that are applicable to all DEA component personnel and a role-based annual privacy training refresher training. There is no additional privacy training specific to this system.

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

Administrative Privacy and Security Controls –All DEA system users are mandated to take annual DOJ Security Awareness Training (CSAT). The implementation of this control helps employees to be informed and be vigilant of any potential cybersecurity concerns that may arise. The training also helps employees to follow the required procedures and report cyber incidents immediately. Least privilege access to the ADAMS system is ensured by assigning the minimum permissions required for users to perform their tasks. Permission and access rights to resources are enforced based on user roles and policies.

Technical Privacy and Security Controls – Logs of system access and administrative actions are maintained to track and review user activities, which helps in identifying and responding to unauthorized access. There will be Access Control Lists (ACL) in place to limit ADAMS traffic to that which originates on Firebird. Firebird is an on-premises/cloud hybrid, General Support System (GSS) environment that is the primary enterprise information technology (IT) infrastructure of the DEA. Firebird provides network infrastructure to host multiple internal DEA systems that reside on Firebird GSS, including ADAMS. ACLs will also apply directly to the systems and clients using ADAMS. Security controls such as access, identification, and authentication controls are utilized. Furthermore, all ADAMS Users gain access via PIV authentication onto the Firebird environment then gain access to the ADAMS software via Single Sign-On (SSO). PIV card and credentials will be received through the standard process. Data integrity is maintained through best practices approaches for data management. This includes efforts for data standardization, data structure (using the relational integrity model), and manual validation processes that exist to ensure integrity of the data at the source of entry. The system's secure internet connection is fortified with advanced encryption and intrusion detection systems, ensuring the integrity and confidentiality of sensitive data.

Physical Privacy and Security Controls – Physical and Environmental controls are enforced across all DOJ's buildings as part of its common control requirements. This is enforced with defense in depth. All DEA buildings are guarded by security personnel at the entrance of the office. Employees are required to be authenticated with their Personal Identity Verification card (PIV) before being granted access to the building. Security Guards are stationed at each DEA facility. Visitors to DEA facilities will be escorted at all times. The physical components of the

ADAMS system necessary for end users to access the viewing and analysis tools are stored in controlled areas and restricted to only authorized FREs.

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.)*

Records are retained and disposed of in accordance with the National Archives and Records Administration's (NARA) General Records Schedule. Latent Fingerprint lab files are maintained under DFN 901-01 (NC1-170-77-1), which provides for transferring case files to the federal records center two years after closing the investigative case and destroying 10 years after the close of the investigative case.

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:*

JUSTICE/DEA-008 Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012), <https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf>.

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).

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 The Collection of the Information.

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

Mitigation: This risk is mitigated. Fingerprints or other friction ridge prints generally are obtained from evidence gathered pursuant to an authorized investigation or, in some cases, where DEA directly collected known prints of persons who appear to be relevant to an

investigation or who are applicants for employment. Information in ADAMS is limited to what is necessary to aid authorized investigations. This includes the friction ridge print images gathered from evidence or directly from individuals and any analysis thereof (i.e., matching the print to other known prints). It also includes known fingerprint cards received from the FBI.

Privacy Risk: DEA may collect PII of an unrelated individual (who is not under suspicion or the subject of investigation) as part of an incident or investigation about someone else and the person to whom the collection pertains may be unaware of and/or unable to consent to DEA's collection of their PII.

Mitigation: This risk is partially mitigated. Another person other than the subject of interest to DEA may leave a latent print on a piece of evidence. For example, a plastic bag from a local grocery store might have the latent prints of both the grocery store employee that bagged the items as well as the subject of interest to DEA who used the plastic bag to transport controlled substances. All print images acquired in ADAMS will be retained according to the NARA retention schedule, even if subsequently identified by a submitting agent as belonging to an individual not presently known to be involved in an investigation. However, the identity of a person who is not a subject of interest to DEA will only become known to DEA if the friction ridge detail is sufficient to put into the FBI NGI database for a search and that person's known prints are in the system. If unidentified prints are retained within NGI's ULF, the DEA FREs have the ability to delete those prints subsequently identified. DEA cannot fully mitigate against this risk and DEA cannot control who might leave latent prints on a piece of evidence. However, only items that are of evidentiary value to an investigation are collected and then later submitted for friction ridge analysis to DEA.

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

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

Mitigation: This risk is mitigated. The prints processed by ADAMS generally are obtained from evidence gathered pursuant to an authorized investigation or in some cases, where DEA directly collected fingerprints of persons who appear to be relevant to an investigation or who are applicants for employment. ADAMS results are sent via LIMS to the case agent requesting the analysis, whereupon the result becomes part of the case file for that investigation.

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 reduced by the administrative, technical, and physical mitigation controls discussed in section 6.2. DEA has developed and enforces comprehensive security policies and procedures such as an Incident response plan and acceptable use policies. To limit the potential for insider threats or technical breach, the system may only be accessed by users with unique and attributable accounts from within government facilities, or by remote access by a limited number of system administrators through VPN connections using a two-factor authentication process.

There are also ongoing security awareness trainings for employees to take annually. Regular audits of user access and permission are conducted to ensure they are appropriate. The principle of least privilege is applied within ADAMS by granting users only the level of access necessary to perform their job functions.

Privacy Risk: ADAMS may retain data longer than necessary, which may reduce the relevance and timeliness of the data.

Mitigation: This risk is not yet mitigated. Data is to be retained in accordance with National Archives and Research Administration (NARA) guidance and instructions, which generally provides that case files are destroyed 10 years after that the close of the investigative case. However, purging data from ADAMS after close of the investigative case would prevent the DEA from identifying subsequent case linkages. DEA is currently working to develop a process to parse and retain unidentified latent prints for comparison in subsequent investigations.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: DEA personnel may access the information without a need to know or disclose PII Information to an inappropriate party or for an improper purpose.

Mitigation: This risk is mitigated. Access to ADAMS is strictly controlled. Only FREs with a need to know are given access to the print images in ADAMS and then document their conclusions based on the print images in DEA's Laboratory LIMS. The need to know is effectuated by limiting access within ADAMS to each user's specifically assigned cases. . The data on ADAMS, such as fingerprint cards when requested as part of an arrest or investigative process, is physically and logically restricted to DEA personnel who have been authorized by the government to have access. Only FREs, DEA-cleared system engineers (contractors), and the program manager are given direct login access to ADAMS. Special agents on the relevant case (i.e., those with a need to know) receive ADAMS data via LIMS in final reports issued by FREs.

The latent prints data are stored in government facilities with access control measures in place. Within these facilities, the physical components of the system necessary for end users to access the viewing and analysis tools are stored in controlled areas and restricted to only authorized Friction Ridge Examiners.

With respect to dissemination to an inappropriate party, as noted above, ADAMS data cannot be directly accessed other than by authorized FREs, contractors and program management. Therefore, any dissemination of ADAMS data would occur only when the final report and associate image is downloaded via LIMS to the case file. If the agents receiving the report further disseminate it, the disclosure would be made from the DEA case files, not ADAMS. Regardless, however, such disseminations are done consistent with applicable laws, regulations, and DOJ policies. Any subsequent dissemination of data originating from ADAMS is governed by the relevant DEA System of Records Notices, DEA privacy guidance, or are authorized by DEA's Office of Chief Counsel for legal and authorized purposes, such as release to a defendant in a criminal case.

Additionally, all DEA employee and contractor users of ADAMS, both administrators and end users, must complete the DEA Cyber-Security Awareness Training and agree to the IT Rules of Behavior for use of DEA information systems every year. The lawfully collected data is logically protected from unauthorized viewing and copying by computer login restrictions which permit only authorized users to have access to the data as well as specific permission-based access restrictions at both the application interfaces and the file level.