Justice Management Division (JMD)

Privacy Impact Assessment
for the
Joint Automated Booking System (JABS)

Issued by:
Morton J. Posner
JMD Senior Component Official for Privacy

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: April 21, 2025

(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 Joint Automated Booking System (JABS) is a system within the Department of Justice (DOJ) Justice Management Division (JMD) Justice Criminal Information Services (JCIS) that provides authorized federal and tribal agencies access to the Federal Bureau of Investigation Criminal Justice Information Systems (FBI CJIS) Division Next Generation Identification (NGI) system[1]. Authorized users of JABS include, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Drug Enforcement Administration (DEA), the FBI, the Federal Bureau of Prisons (BOP), and the U.S. Marshals Service (USMS). This allows authorized users to submit biographic and biometric data (fingerprints, palm prints, iris photos, face photos, scars, marks, tattoos) and receive the expedited return of an offender's national Identity History Summary (IdHS) information (a.k.a. Rap Sheet), including applicable Department of Homeland Security (DHS) Automated Biometric Identification System (IDENT)[2] , immigration information and/or presence of DNA in the Combined DNA Index System (CODIS)[3]. JABS also stores biographic and biometric data to support continued information-sharing efforts between authorized agencies and national investigative information systems, such as the FBI National Data Exchange (N-DEx)[4]. JABS reduces duplicative bookings of offenders for a single arrest or booking, and thereby largely eliminates the collection of the same data by multiple agencies. In addition, JABS standardized booking data elements enable interagency sharing of booking information, enhancing cooperation among law enforcement agencies, and reducing the threat to law enforcement officials and the public by facilitating the rapid and positive identification of offenders.

This PIA has been prepared to address the use of additional biometric data enhancements leveraged by JABS (i.e., facial recognition technology (FRT), iris images, and DNA sample collections).

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.

JABS is a system that allows authorized User Agencies to (1) capture biometric and biographical data through a client-based application which automates and accelerates the booking process, and (2) enable authorized entities to access or submit booking information for criminal investigations and other law

[1] NGI is covered by separate privacy documentation. See https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments.
[2] IDENT is covered by separate privacy documentation. See https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.
[3] CODIS is covered by separate privacy documentation. See https://www.fbi.gov/file-repository/pia-combined-national-deoxyribonucleic-acid-dna-index-system-codis-031423.pdf/view.
[4] N-DEx is covered by separate privacy documentation. See https://www.fbi.gov/file-repository/pia-national-data-exchange-n-dex-system.pdf/view.

enforcement activities. Authorized users can leverage JABS to:

- Submit electronic booking packages for offenders to create new criminal history records in the FBI NGI system and allow for enrollment of fingerprints, palm prints, face, iris, scars, marks, and tattoo images;
- Submit electronic fingerprint packages to perform identity verification on subjects;
- Submit DNA sample collection kit barcode information, automate creation of the Request for National DNA Database Entry FD-936 form and view the status of existence of a DNA profile in CODIS) for subjects;
- Generate investigative leads by submitting a frontal face probe photograph via the JABS pass-through service to NGI to conduct Facial Recognition Searches (FRS) (JABS presents the NGI response of up to 20 potential image matches to the submitting organization's trained facial recognition examiners for review); and
- The JABS Web Tool, which is accessible via DOJ Login[5] and the FBI's Law Enforcement Enterprise Portal (LEEP)[6] only, allows authorized users to conduct queries to view arrest, booking, and criminal history information.

Captured offender data is consolidated into an Electronic Fingerprint Transmission (EFT) package that is transmitted via email or web service to JABS[7], which automatically validates the data to ensure it meets the requirements as detailed in the FBI's CJIS Electronic Biometric Transmission Specification (EBTS), and transmits it to FBI NGI. After NGI has received the information, the FBI will search against its database for a match. Should the match occur, the FBI Number, IdHS, and any other fingerprint or identification information will be transmitted back to JABS. When no match occurs for the offender's fingerprints, the NGI response will state that the offender has not been identified within NGI.

JABS maintains data logs for User Agencies and individual authorized users for audit and administrative purposes, and these logs are accessible to the DOJ Office of the Chief Information Office (OCIO) CJIS Systems Agency (CSA) during routine audit cycles. Authorized users are determined by the User Agency's Terminal Agency Coordinator (TAC) and governed by the DOJ CSA User Agency Agreement (UAA); all TAC responsibilities are outlined in the UAA and the TAC Addendum. Authorized users are required to complete CJIS Security Awareness Training (CSAT) annually as part of the agreement.

JABS supports the following DOJ mission-critical services:

- Protect the United States from terrorist attacks and foreign intelligence operations and espionage; share law enforcement information with authorized federal and tribal agencies, as necessary to investigate/prosecute terrorists, foreign agents, and organizations that threaten the United States.
- Conduct federal law enforcement activities and coordinate federal law enforcement response as needed in national and international emergencies.
- Operate the federal detention and prison systems to ensure the continued confinement of prisoners.

---

[5] DOJ Login is covered by separate privacy documentation, *see*: https://www.justice.gov/d9/2024-04/pia-jmd-doj_login_final.pdf.
[6] LEEP is covered under separate privacy documentation, *see*: https://www.fbi.gov/file-repository/pia-leep-070319.pdf/view.

7 Most JABS customers submit EFT files via e-mail to NGI. Once NGI receives the e-mail submission from JABS, it processes it via their system. The JABS to NGI interface is e-mail based. NGI does not manually enter data. It is processed automatically via systems they have in place. In some limited circumstances, JABS customers leverage a web service to submit the EFT files to JABS for NGI processing (utilizing hypertext transfer protocol secure (HTTPS) and machine-to-machine interactions).

- Equip the Department's law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the United States while preserving civil liberties.

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	28 U.S.C. § 534; 8 U.S.C. § 1357(f)-(g) 28 U.S.C. §§ 564 and 566 5 U.S.C. § 301 5 U.S.C. § 552a; 44 U.S.C. § 3101; 18 U.S.C. § 4082
Executive Order	Executive Order 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety, Secs. 13(e) and (f).
Federal regulation	28 C.F.R. § 20.33
Agreement, memorandum of understanding, or other documented arrangement	UAAs are in place with each entity that uses JABS for submissions.
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non- USPERs	(4) Comments
Example: Personal email address	X	B, C and D	Email addresses of members of the public (US and non-USPERs)
Name	X	A, B, C and D	
Date of birth or age	X	C and D	
Place of birth	X	C and D	
Sex	X	C and D	
Race, ethnicity, or citizenship	X	C and D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Full Social Security Number
Tax Identification Number (TIN)			
Driver's license	X	C and D	
Alien registration number	X	C and D	
Passport number	X	C and D	
Mother's maiden name	X	C and D	
Vehicle identifiers	X	C and D	
Personal mailing address	X	C and D	
Personal e-mail address			
Personal phone number	X	C and D	
Medical records number			
Medical notes or other medical or health information	X	C and D	
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information (*Occupation Position*)	X	C and D	

(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	X	C and D	
Juvenile criminal records information	X	C and D	JABS authorized users can indicate if an arrestee is a juvenile and/or if they are a juvenile to be Treated as an Adult when submitting booking packages.
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			
Location information, including continuous or intermittent location tracking capabilities			
Employing Government Agency	X	A and B	JABS stores the Government Agency information for authorized users.

(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
Address of Government Agency	X	A and B	JABS stores the Government Agency address for authorized users.
Biometric data:			
- Photographs or photographic identifiers	X	C and D	
- Video containing biometric data			
- Fingerprints	X	C and D	
- Palm prints	X	C and D	
- Iris image	X	C and D	
- Dental profile			
- Voice recording/signatures			
- Scars, marks, tattoos	X	C and D	
-Vascular scan, e.g., Palm or finger vein biometric data			
- DNA profiles			
- Eye Color	X	C and D	
- Height	X	C and D	
- Weight	X	C and D	
System admin/audit data:	X	A and B	JABS collects audit data for privileged (JABS systems administrators) and non-privileged user actions within the system (discussed below in section 6.2).
- User ID	X	A and B	
- User passwords/codes	X	A and B	
- IP address	X	A and B	
- Date/time of access	X	A and B	
- Queries run	X	A and B	

(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
- Contents of files	X	A and B	
- Name	X	A and B	
- Email Address	X	A and B	
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

To avoid confusion, the table below has been filled in only regarding the "substantive" information maintained by JABS – the information pertaining to suspects or criminals – not the user registration and audit information maintained on JABS account holders for administrative purposes (which is collected either directly from the user or from the user's agency). JABS itself does not collect any of the substantive information directly from the suspect or criminal; that information is collected by agency booking systems (whether directly from the suspect or criminal, or from other sources), which electronically transmit the information to JABS.

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
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):					

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	Authorized DOJ JMD JABS users can access JABS data via a secure web portal (JABS Web Tool) using direct login access provided by DOJ Login.
DOJ Components		X	X	JABS arrestee data is forwarded to NGI via secure system generated email. NGI responses are processed via JABS and forwarded to ATF, FBI, and DEA via secure email. Arrestee data and NGI responses are sent bidirectionally between JABS and USMS/BOP via secure web services. JABS conducts a bulk electronic transfer nightly to the FBI's N-DEx system and the Organized Crime Drug Enforcement Task Force (OCDETF) containing all the previous days' arrest records using a National Information Exchange Model (NIEM) Extensible Markup Language (XML) format.

				Authorized ATF, BOP, DEA, FBI, and USMS users can access JABS data via a secure web portal (JABS Web Tool) using direct login access provided by DOJ Login.
Federal entities			X	JABS arrestee data is forwarded to NGI via secure system generated email. JABS arrestee data and NGI responses are sent bidirectionally using secure email between JABS and authorized federal agencies. Authorized federal law enforcement agency users can access JABS data via a secure web portal (JABS Web Tool) using the FBI's Law Enforcement Enterprise Portal (LEEP).
State, local, tribal gov't entities			X	JABS arrestee data and NGI responses are sent bidirectionally using secure email between JABS and authorized tribal law enforcement agencies. Authorized tribal law enforcement agency users can access JABS data via a secure web portal (JABS Web Tool) using LEEP.
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.

Information in JABS will not be released to the public.

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.

Information in this system is collected during law enforcement activities and individuals generally do not have the opportunity to decline to provide information. The Department has published a Privacy Act SORN, Nationwide Joint Automated Booking System, DOJ-005, 71 FR 52821 (9-07-2006) for records maintained in JABS (E6-14828.pdf (govinfo.gov)) which provides generalized notice to the public about why information is collected for JABS and how the information is being used. This PIA also provides general notice, as does the previously published PIA regarding JABS, which may be found at: Joint Automated Booking System (justice.gov).

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 JABS, as the information collected in this system is done so during law enforcement activities. An individual whose biometrics are collected during a criminal or national security investigation has no choice to refuse the collection of their biometrics. In addition, information in this system is exempt from the access and amendment provisions of the Privacy Act, as well as certain notice provisions of the Act such as subsection (e)(3), pursuant to subsections (j)(2) and (k)(2) of the Act (*See* 28 C.F.R. § 16.131).

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.

JABS collects and stores information related to criminal bookings, if individuals need to correct or amend information pertaining to them, they must request an amendment or correction within the FBI NGI system per FBI CJIS procedures as outlined in Section 5.3 of the NGI Biometric Interoperability PIA:

> *The FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records maintained in the NGI System. However, title 2 CFR part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; and 28 CFR part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files to the extent it is available pursuant to the Privacy Act. In addition, title 28 CFR 16.20-16.34 establishes specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction.*

Should FBI CJIS correct, amend, or expunge a record in the NGI system, FBI CJIS will communicate the details of the change to JABS via a Records Modification Request. JABS Program/Helpdesk will process the Records Modification Request to update the record accordingly within JABS.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** The most recent ATO for JABS was issued on 9/13/2024 with an expiration date of 9/13/2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	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:** Per the FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, JABS has been assigned a security categorization of Moderate. As detailed in the JABS Security Plan (SSP), JABS was determined to be a Moderate level after reviewing the information types with respect to their Confidentiality, Integrity, and accessibility (CIA) ratings. All information types were assessed at either Low or Moderate which contributed to the overall security categorization of Moderate for the system.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** To safeguard information, JABS leverages security tools to proactively monitor network traffic for signs of potential malicious activity and uses software to protect endpoints from threats in real-time. Additionally, audit logging is in place on records within JABS to help prevent its misuse. Prior to release, new functionality is developed and tested in separate

	development, test, and pre-production environments. Per UAAs, agencies must follow the FBI CJIS Security Policy. According to the DOJ CSA UAA TAC Addendum, TACs must also report suspected or verified misuse of FBI CJIS systems to the CSA. The CSA notifies the JABS Incident Response Team which, in turn, will notify the DOJ Service Desk and/or the DOJ's Justice Security Operations Center (JSOC). The JABS Incident Response Team will initiate an investigation and perform an evaluation of potential security violations and impacts according to the JABS Incident Response Plan. Additionally, information contained within JABS uses industry standard encryption both at rest and in transit. JABS also creates an audit trail by logging non-privileged user interactions within the system including logins/logouts, records entered, searches conducted, and records viewed. Privileged user access is limited with additional auditing mechanisms in place to include administrative interactions within JABS such as account creation/modification/deletion requests and record modifications. Privileged user roles and permissions are reviewed on a monthly basis by the JABS Service Owner.
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:** JABS logs are forwarded to DOJ's system event data repository and are reviewed weekly by the JABS Information System Security Officer (ISSO) per CJIS Security Policy section 5.4.3. Vulnerability scans are routinely conducted to identify whether there are any weaknesses which can be exploited for unauthorized intrusion. The JABS program reviews vulnerability scan results weekly.
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 contractors are required to take annual cybersecurity awareness training and privacy training as provided by their agency. All contractors, regardless of their agency, must complete annual CJIS Security Awareness Training and must sign the CJIS Security Addendum and CJIS Handling Addendum.
X	**Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All authorized JABS users and privileged users must complete required CJIS Security Awareness Training prior to being granted access to JABS and data within.

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?

The primary transmission method of biometric submissions to JABS is electronically (via email and web

service(s) note in footnote 7, above) via the DOJ's Justice Unified Telecommunications Network (JUTNet). JUTNet is a telecommunications infrastructure that is DOJ's Wide Area Network and provides a secure and encrypted transport mechanism for JABS biometric and criminal history records information. JUTNet is configured by DOJ personnel and secured through cybersecurity mandates. Authorized non-DOJ User Agencies connect to JABS services via the Law Enforcement Enterprise Portal (LEEP)[8] interface which leverages Multi-Factor Authentication (MFA). MFA acts as an additional layer of security to validate user identities, provide access to authorized users, and prevent unauthorized users from accessing these accounts.

Biometric transactions submitted to JABS are compliant with the FBI's EBTS. The EBTS ensures compatibility with JABS and the FBI's NGI system, and the American National Standards Institute/National Institute of Standards Technology – Information Technology Laboratory (ANSI/NIST-ITL) standard. ANSI/NIST-ITL is developed and maintained in conjunction with NIST and the biometric community. While the ANSI-NIST-ITL standard provides guidelines for the exchange of information systems between various federal, state, local and tribal biometric systems, the EBTS defines requirements to which agencies must adhere when electronically communicating with the JABS and the FBI's NGI system.

JABS provides access to information via three defined roles: Non-Privileged User, TAC, and Privileged User. As defined in the UAAs and according to CJIS Security Policy, TACs manage their respective agency's Non-Privileged User Accounts (i.e., account management for general users who can submit transactions to JABS and query the system). Privileged Users (e.g., system administrators) have elevated access rights to view data as necessary to manage the system, manage user accounts, etc..

System audit logs record and capture actions taken within a system, along with details that allow tracking those actions back to the individuals who performed them. All system audit data is stored according to DOJ retention polices and guidelines, discussed below.

Only authorized criminal justice agencies may search and retain biometric and criminal history data within JABS. Authorized JABS User Agencies must ensure compliance with CJIS Security Policy and applicable JCIS User Agreements. The CJIS Security Policy governs the information security requirements for the NGI system, including JABS, which acts as a gateway for Authorized User Agencies to access the NGI system. The DOJ CSA User Agency Agreement specifies that agencies are responsible for complying with the CJIS Security Policy to ensure they adhere to requirements for physical security, technical security, and personnel security, as well as user authorization and dissemination. The system stores information regarding dissemination, such as date, time, and requestor in audit logs. Risks are also mitigated by training, annual account re-certification following the Law Enforcement Services and Information Sharing Account Validation Process, and user compliance with DOJ Rules of Behavior agreements.

User Agencies and their users are not authorized to access JABS, or the JABS Web Tool without an Originating Agency Identifier (ORI) issued by CJIS. Access to the NGI is essentially restricted to criminal justice agencies that perform the administration of criminal justice as defined in 28 C.F.R. § 20, Subpart A. CJIS approved and assigned ORIs will provide the correct level of access to CJIS systems. ORI access is strictly controlled and audited by CJIS.

In addition, the JABS ISSO is responsible for ensuring the overall operational security posture is

[8] LEEP is covered by separate privacy documentation. See https://www.fbi.gov/file-repository/pia-leep-070319.pdf/view.

maintained on a day-to-day basis for JABS. Adherence to roles and rules is tested as part of the system security certification and accreditation process. All JABS employee and contractor personnel must complete Privacy Training provided by DOJ Office of Privacy and Civil Liberties, DOJ Records and Information Training, Information Technology Professional Training for Privileged Users, CSAT, and CJIS Security Awareness Training.

In accordance with 28 U.S.C. § 534, DOJ does not disclose information from JABS outside of the authorized receiving agency or related agencies. This statute provides specific controls on the dissemination of criminal history record information, including identification of authorized recipients and potential sanctions for unauthorized disclosures. In addition, authorized users must comply with applicable security and privacy protocols addressed in the latest published version of the CJIS Security Policy.

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.)

Pursuant to DOJ Order 0904, Cybersecurity Program, JCIS implements the data minimization and retention requirements, which states that components will only retain PII that is relevant and necessary for the purpose for which it was originally collected. JCIS uses the National Archives and Records Administration's General Records Schedule 3.2 Information Systems Security Records and 4.2 for Information Access and Protection Records to determine how long the records should be retained before disposition. Additionally, the CJIS Security Policy requires logs of records be retained a minimum of one year.

On occasion, an expungement order might apply to information in a booking record. When the order is communicated to FBI's CJIS, CJIS sends a record modification request to the JABS Program for evaluation. The Program's Help Desk Lead will then expunge the record in accordance with the expungement order.

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:

A System of Record Notice (SORN) exists for JABS:

Number: DOJ-005
System Title: Nationwide Joint Automated Booking System (JABS)

SORNs:

- 71 FR 52821 (9-07-2006)
- 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147)
- 82 FR 24127 (5-25-2017)

Exemptions:

- Exemptions Claimed Pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). See 28 C.F.R. § 16.131

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:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

JABS collects information submitted by authorized users for the purpose of populating the NGI system with arrest and booking event information as well as processing EBTS packages for subject identification.

The risk of JABS information being used by unauthorized persons or for unauthorized purposes has been greatly mitigated by technical and policy safeguards. The types of data, the criminal law enforcement purposes, and requirements for access and dissemination of JABS data are described in Section 2 of this PIA. Technical safeguards deployed to protect JABS information are described in Section 6, above.

JABS data can be queried by trusted law enforcement partners that are also subject to the Privacy Act of 1974 in addition to other relevant federal laws, statutes, and executive orders. Data sharing between JABS and other agencies is in accordance with Interagency Security Agreements (ISAs) and UAAs. The ISAs and UAAs ensure that only the minimum mission relevant data is collected and shared.

Usage of JABS FRS features requires prior authorization to allow users to submit probe photographs to generate investigative leads. JABS FRS users must be trained by the FBI, or an FBI-approved training provider. The FBI Face and Identification Training includes steps to develop conclusions (Likely Candidate, Inconclusive, or Eliminated) when reviewing and comparing a result set against the original probe image. JABS users are informed that candidate photos returned are provided as investigative leads only and are not to be considered positive identification.

Only authorized users from approved law enforcement organizations can access JABS data. These users are governed by rules of behavior and must comply with routine training and certification. Additionally, auditing is in place to track user interactions within JABS. Further, account management policies and procedures are in place to automatically deactivate unused accounts after defined criteria are met.

By Department Order, all DOJ users with access to Department networks, including JABS, must take the annual CSAT course. This course includes information on federal information privacy laws, such as the Privacy Act and requirements for proper handling of PII. The course also identifies potential risks and vulnerabilities associated with using DOJ-owned information technology systems, reviews the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course.

Privacy risks are further reduced, for User Agencies that contribute, through processes and policies in place by the agency for accessing and the correction of source records in the NGI, as referenced in Section 5.3 above.