Justice Management Division (JMD)

Privacy Impact Assessment
for the
Joint Automated Booking System

Issued by:
Arthur E. Gary, General Counsel, JMD

Reviewed by: Luke J. McCormack, Chief Information Officer, Department of Justice

Approved by: Joo Y. Chung, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date originally approved: January 21, 2002
Date revision approved: May 6, 2013

(September 2012 DOJ PIA Form)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) posted at http://www.justice.gov/opcl/pia.htm.]

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;

The Joint Automated Booking System (JABS)[1] is an information-sharing system as well as a conduit for sending standard booking data directly to the Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS). JABS receives common offender data elements (biographical data, fingerprints, and photographs) from automated booking stations and booking systems of DOJ law enforcement components and certain other federal law enforcement agencies and maintains a shared repository that can be accessed by all participating agencies. JABS is governed by the JABS Board of Directors and managed by the JABS Program Management office, within the Justice Management Division of DOJ.

The purpose of JABS is to (1) automate and accelerate the booking process, and (2) enable authorized entities to access booking information for criminal investigations and other law enforcement needs. Sharing booking data allows investigative agencies to identify arrested persons quickly, reduce redundant data entry, and track offenders from booking through disposition. Records can be amended by participating agencies as the situation, personal data, or geographic location change. JABS also provides agencies with connectivity needed to submit fingerprints to IAFIS electronically and receive the resulting fingerprint and offender identification and criminal history findings. All communications are supported by the Justice Consolidated Network (JCON) and FBI Criminal Justice Information Services (CJIS).

Since the last JABS PIA was approved, in 2002, the data collected and uses of the data have remained largely unchanged. This PIA is being revised because other, non-DOJ federal agencies, as well as some state and local law enforcement agencies, are being added to the categories of users (although the state and local users will only have read/query/investigatory access, not the ability to create booking records, as explained below). In addition, the PIA is being updated to document the privacy-related consequences of recent system enhancements. These enhancements have enabled more precise interoperability and information governance, as described below in sections 3.2 and 4.

[1] There are 2 major subsystems that fit under the umbrella known as Joint Biometrics Data Exchange Hosting Environment (JBDEHE): JABS and the Civilian Applicant System (CAS). This PIA covers JABS; the PIA for CAS is posted at: http://www.justice.gov/opcl/pia.htm. Note that in this document, for the purpose of maintaining historical convention, the program running JBDEHE is still referred to as the "JABS Program."

(b) the way the system operates to achieve the purpose(s);

The operational workflow of JABS begins with the arrest of a suspect by a federal law enforcement agency. Using its own booking system, the agency collects booking information (including both identifying information and arrest-related information, as described in section 2) and creates a file for the information, called a booking record. The agency then sends the booking record to JABS via secure electronic message transported by JCON. JABS validates each booking package and forwards digital fingerprints to IAFIS for identification. IAFIS determines whether the individual has a criminal history; if so, then IAFIS sends this information (the "rap sheet") to JABS, where this criminal history information is collated with the individual's booking record. If the individual has been previously booked as a federal prisoner, then IAFIS will send JABS the FBI number assigned to that individual. If the individual has never been booked as a federal prisoner, then IAFIS will create an FBI number for the individual and send it to JABS. Once JABS receives the FBI number, the booking record is complete. JABS then forwards a copy of the rap sheet and any other fingerprint or identification information from IAFIS to the originating law enforcement agency.

Authorized JABS users may access the JABS database through a secure connection to JCON using their agencies' booking stations or a web browser. Users may then retrieve booking information – by known offender characteristics such as name, social security number, date of birth, or vehicle license number – for criminal processing purposes or for intelligence or investigative purposes. Users can then view and print the offender summary, personal history report, booking history, and photographs. Downstream processing agencies, such as the U.S. Marshals Service (USMS), and the Federal Bureau of Prisons (BOP), access JABS to capture the online booking package and FBI response in order to create their own agency-unique database records on the offender.

(c) the type of information collected, maintained, used, or disseminated by the system;

JABS maintains arrest information as well as biographical and biological information about individuals, as listed in section 2.1 and Appendix A. The system also collects and maintains user information, including user registration information (e.g., name, work contact information), authentication information (e.g., user ID), and audit log information.

(d) who has access to information in the system;

The following categories of users have access to JABS:

- <u>Operators</u>: Law enforcement agency personnel who have read and write access, for the purposes of allowing them to create booking records as well as query information already stored in the JABS database.
    - List of entities with operators accessing JABS: Bureau of Prisons (BOP); Drug Enforcement Administration (DEA); U.S. Marshals Service (USMS); Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); Federal Bureau of

    - Investigation (FBI); Department of Homeland Security (DHS) (Immigration and Customs Enforcement (ICE); Customs and Border Protection (CBP); and Secret Service); Pentagon Police; U.S. Park Police; National Park Service; Administrative Office of U.S. Courts; and Department of Defense (DoD)
- Investigators: Law enforcement agency personnel who have only read access (via the online query tool), allowing them to query information already stored in JABS for investigative purposes.
    - List of entities with investigators accessing JABS: BOP; DEA; USMS; ATF; FBI; DHS (ICE; CBP; and Secret Service); Pentagon Police; U.S. Park Police; National Park Service; Administrative Office of U.S. Courts; Department of Defense; and state and local law enforcement agencies.
- Administrators: Federal or state/local government personnel and contractors who provide technical support and who may access JABS for the purpose of performing maintenance, troubleshooting, or performing enhancements.
    - JABS personnel, who consist of JMD employees and contractors.
- Local area coordinators: Individuals who are responsible for enrolling new users.
    - JABS is moving toward having a local area coordinator (LAC) at each federal agency. Currently, though, DEA and DHS are the only federal agencies with active LACs.

It is expected that access to JABS will gradually be expanded to additional non-DOJ federal agencies. This is because, as stated above, JABS is one of the main conduits for sending fingerprints and other standard booking information to IAFIS through CJIS (though it is not the only such conduit), and because CJIS is requiring electronic submissions instead of paper submissions. (JABS sends booking data to CJIS in the form of Electronic Fingerprint Transmission Specification (EFT) files, but CJIS personnel do not have direct access to JABS.)

In addition, specific extracts of JABS data may be provided to law enforcement agencies upon request, subject to the JABS rule of behavior. (The rules of behavior provide that JABS data may only be used for official criminal justice purposes or in support of authorized investigative activities.) The following entities receive extracts of JABS data: DEA; Pinellas County Florida; the U.S. Department of Justice's Organized Crime and Drug Enforcement Task Force (OCDETF); and the Arizona Counter Terrorism Information Center (ACTIC). (The extracts are specific subsets of JABS data deemed necessary by the requesting organization to assist in its operations.)

Finally, note that permissions can be assigned on a line-item basis, and that all authorized users have agreed to the JABS rules of behavior.

(e) how information in the system is retrieved by the user;

The query tool is used to retrieve information by any database field. Users who receive extracts of JABS information retrieve information by any database field in the extract. Rap sheets are retrieved by submitting a suspect's fingerprints to JABS.

(f) how information is transmitted to and from the system;

Information is transmitted to and from the system via encrypted web services, secure e-mail, and file transfer protocol (FTP) (a method of transferring files across a network between computers).

(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and

JABS has nine major interfaces – five external and four internal. The first is a generic interface between JABS and a law enforcement agency's booking stations. The second is the interface between JABS and IAFIS. The third is the JABS web interface between JABS and an end user. The fourth is the internal web service and web interfaces between JABS and USMS. The fifth interface is internal and provides a daily FTP push to OneDOJ (a criminal law enforcement data repository). The sixth interface is internal and provides data to OCDETF via e-mail with file attachments. The seventh interface is internal and provides data to DEA via e-mail with file attachments on a monthly basis. The eighth interface is external and provides data to ACTIC via FTP to a JCON-hosted FTP server with file attachments on a weekly basis. The ninth interface is external and interfaces with the query tool to the Chicago Police Department's Investigative Resources System.

(h) whether it is a general support system, major application, or other type of system.

JABS is a major application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration	X	Financial account	
Taxpayer ID		Driver's license	X	Financial transaction	
Employee ID		Passport	X	Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify): FBI number; state identification number; vehicle identification number; license plate number; visa number; arrest identification number; military identification; U.S. Marshals Service number; BOP register number					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth	X	Financial info	
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	

General personal data					
Age	X	Email address		Physical characteristics	X
Race/ethnicity	X	Education		Mother’s maiden name	
Other general personal data (specify): Marital status; citizenship status (as well related information, e.g., visa type, visa number, country of citizenship); criminal history					

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title		Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify): Email address collected only from authorized users; name of employer					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): Height; weight; eye color; hair color; missing limbs; facial features					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run	X	Contents of files	X
Other system/audit data (specify): Transaction ID (number assigned to booking transactions); user registration information (e.g., name, contact information, user ID, password)					

Other information (specify)
Vehicle information (e.g., make, model, year, color, state, identification number, license plate number, drivers license number); names of associates; prescription drugs used by suspect; arrest information (e.g., time, date, location); date of offense; jail location; charge; disposition; and any other pertinent information related to known activities relevant or unique to the subject (as stated in the JABS system of records notice, 71 Fed. Reg. 52821 (Sept. 7, 2006)).

(See also Appendix A.)

2.2 Indicate sources of the information in the system. (Check all that apply.)

To avoid confusion, the table below has been filled in only with regard to 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 individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

As described above, JABS was designed to streamline the booking process as well as to promote the information sharing of booking data to authorized law enforcement agencies. Because this system maintains sensitive criminal justice data, privacy concerns include the unauthorized access and disclosure of this data, proper data quality and appropriate reliance on the data within the system, and concerns regarding appropriate data minimization and effective notice to the subject individual.

With regard to proper access to JABS data, the JABS Program only permits access to authorized law enforcement agencies who have accepted the rules of behavior regarding the proper use and handling of JABS data, and who have a need for the information for a law enforcement purpose. As mentioned above, the JABS rules of behavior provide that JABS data may only be used for official criminal justice purposes or in support of authorized investigative activities. Local agency coordinators are responsible for approving all new users and ensuring that they have a need-to-have access to JABS for such purposes. The principal agency JABS liaison is responsible for recertifying all active JABS users annually to ensure that users have the appropriate level of access to JABS.

Access is immediately terminated when the individual leaves the agency or no longer requires access to the system. Therefore, even though JABS maintains a significant amount of sensitive personal information, the Department has implemented controls to help protect the integrity of the information, and guard against improper access to or misuse of the information.

Data quality and reliance on accurate data are also important privacy concerns with regard to information maintained in this system. Although the information maintained by JABS is technically not collected directly from the subjects of the information (i.e., suspects or criminals), JABS receives this information directly from agency booking systems, which collects certain information directly from its subjects, thereby, reducing the risk of inaccurate data collected and associated with the subject individual. In addition, agency personnel who create booking records are responsible for ensuring that the information is valid and accurate when they transmit it to JABS as they manually enter the data from internal forms.

Once the JABS data is transmitted to IAFIS through CJIS, it is matched with FBI data, as described above. Specifically, information not entered by the booking agency (e.g., FBI number, criminal history information) is provided by CJIS; JABS automatically updates booking records with such information. For example, when a new suspect is booked and the booking record is entered into JABS, that booking record is assigned an FBI number, which is added to the booking record itself. Any criminal history information about the individual is also added to the booking record. These procedures help ensure the completeness, timeliness, and accuracy of JABS data.

Furthermore, the collection of JABS data in the system is minimized at the point of entry as not all data fields, as described in Appendix A, are mandatory. Agencies that submit booking records have discretion regarding whether or not to fill in many of the fields. Mandatory fields (e.g., fingerprints, booking date, booking time, JABS transaction ID number, FBI number (if applicable)) are fields that IAFIS requires in order to process a booking record. (Agencies that submit booking records may require that additional fields be filled in.) JABS validates booking package submissions to ensure that all mandatory fields are filled in. The fact that only certain fields are mandatory reduces the risk that a particular item of information will be inaccurate, and in the event that the system is compromised, fewer items of information are likely to be disclosed.

Finally, as described more fully in Section 5, information in this system is collected during law enforcement activities and individuals and the public are provided general notice of information in this system by the Privacy Act system of records notice published at 71 Fed. Reg. 52821 (Sept. 7, 2006); 72 Fed. Reg. 3410 (Jan. 25, 2007) (modification), which promotes transparency about the uses and purposes of the information that is maintained in JABS.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities		For civil enforcement activities

	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

Information is collected by federal law enforcement agencies (namely, FBI, DEA, ATF, U.S. Park Police, Pentagon Police, Secret Service, Department of Homeland Security, Administrative Office of the U.S. Courts, and Department of Defense) and then transmitted to JABS in order to book individuals (i.e., "to get them into the system"). While these agencies use JABS primarily to complete a booking package, they also use information maintained in JABS to: retrieve the criminal history of the individual; be informed of any danger the individual might present to agency office personnel; and be informed of any medical conditions which require treatment while being held within the criminal processing environment.

JABS users also use JABS information to assist in investigations. For example, vehicle information, physical characteristics, and known associates are valuable for tracking suspects. The information can also be used to verify whether a captive is providing correct information, whether there are outstanding warrants, and other information to help a field agent holding a suspect.

USMS uses the information to track the individual through the court system (in particular, when the individual is held in temporary cells, when custody is transferred from one court to another, or to a prison when the individual enters the corrections portion of the criminal justice process). BOP uses JABS to confirm prisoner identity and to send updates of prisoner location to the Interstate Identification Index (CJIS and National Crime Information Center).

JABS facilitates all of the above functions by serving as a shared repository of information.

Finally, user-related information maintained by JABS is used to manage user accounts, correct errors in data entry, perform audits, and satisfy system security requirements.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	28 U.S.C. § 534; see also 8 U.S.C. §§ 1324, 1357(f)-(g); 28 U.S.C. §§ 564, 566; 5 U.S.C. § 301; 44 U.S.C. § 3101; 18 U.S.C. §§ 3621, 4003, 4042, 4082, 4086; 26 U.S.C. § 7608; Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. No. 91-513), 21 U.S.C. § 801 et seq.; Reorganization Plan No. 2 of 1973 (Pub. L. No. 93-253)
	Executive Order	
	Federal Regulation	
X	Memorandum of Understanding/agreement	MOUs are in place with each entity that uses JABS.
	Other (summarize and provide copy of relevant portion)	

3.4 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.)

JABS information will be retained for 99 years in accordance with an approved National Archives and Records Administration retention schedule.

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.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There are both human threats and technical/electronic threats to privacy and disclosure of personal information maintained in JABS. Many of the human threats and controls in place to mitigate these threats are discussed in section 2.3. These threats include inappropriate dissemination of information or inappropriate use of information. As discussed in section 2.3, controls in place to mitigate these threats include acceptance by all users of rules of behavior; procedures for approving new user accounts and ensuring users' need to know information; regular reviews of user accounts to ensure that users continue to have the appropriate level of access; and immediate termination of accounts when users leave their agency or when they no longer require access to the system.

Technical/electronic threats typically result from vulnerabilities in the system's architecture (including both software and hardware) or deficiencies in security controls, which may allow hackers and other unauthorized users to gain access to the system. Compliance with applicable security standards, including the certification and accreditation process and Federal Information Security Management Act requirements, mitigates these risks. Specifically, a number of technical and architectural controls have been built into the system's architecture in order to mitigate these threats. These controls include:

- Network security
  - The security hardware and software includes seven components: a virtual private network, a screening router, two firewalls, hostile code detection, intrusion detection and an SSL accelerator. These components provide multiple layers of security protection and monitoring. Authorized individuals within the JABS technical staff wear beepers to receive real-time alerts of intrusions.
- Application security
  - JABS security includes access control based on the user ID and password. Auditing features include user and IP address identification, date, time, and data accessed.
  - JABS maintains user IDs, email addresses, passwords for all users, and ORI code (a location identifier) permissions in an Oracle database.
  - Passwords expire in accordance with JABS security standards. Users who fail to change their passwords upon expiration are prevented from submitting packages to IAFIS. An administrator's action is necessary for the re-establishment of the account.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component		X		To OneDOJ, as described in section 1(g).

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
DOJ components			X	While certain DOJ components have direct access to JABS, OCDETF only receives extracts[2] of JABS data.
Federal entities			X	
State, local, tribal gov't entities			X	Some state, local, and/or tribal gov't entities (e.g., ACTIC, Pinellas County) also receive extracts of JABS data.
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			As explained at 71 Fed. Reg. 52821 (Sept. 7, 2006), where necessary and appropriate, the Department reserves the right to disclose relevant information from the JABS repository and may allow electronic access consistent with the routine uses of DOJ-005.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

As described above, the JABS rules of behavior provide that JABS data may only be used for official criminal justice purposes or in support of authorized investigative activities, and they also set forth security rules. The JABS Program only allows access to authorized law enforcement users who have accepted the rules of behavior, and who have a need for the information for a law enforcement purpose. The rules of behavior also provide that unauthorized or improper release of JABS data may violate federal, state, or local laws or Department policy, and they require that an accounting must be

[2] Extracts should not be confused with bulk transfers. As explained in Appendix A, extracts are subsets of JABS information deemed necessary by the recipient agencies for their operations.

kept of secondary dissemination of JABS data (i.e., dissemination of JABS data outside the receiving agency to an authorized recipient).

In addition, Memoranda of Understanding (MOUs) are in place with each agency or component that has access to JABS information. These MOUs are updated periodically as necessary. The JABS MOUs cover the following:

1. Change control (which is how system changes will be documented and managed)
2. Services offered by JABS
3. Interconnection roles and responsibilities; retention /destruction
4. Security policies
5. Contact list
6. JABS end user enrollment process/form
7. JABS end-user rules of behavior statement
8. Interconnection security agreement (ISA)

Please see sections 2.3 and 3.5 for additional information. Additionally, as explained in section 1, some users receive information via the query tool instead of "operator" access to the JABS system. This reduces privacy risk by limiting the number of users who can enter and modify data.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Because JABS itself does not collect information directly from the individual (i.e., suspect or criminal); agency booking systems collect the information from the individual and transmit it to JABS.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: As indicated above, JABS itself does not collect information directly from the individual (i.e., suspect or criminal); agency booking systems collect the information from the individual and transmit it to JABS. Moreover, giving individuals the opportunity to consent to particular uses of the information would significantly interfere with the law enforcement process as the individual progresses through the justice system.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

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 System of Records Notice (SORN), 71 Fed. Reg. 52821 (Sept. 7, 2006); 72 Fed. Reg. 3410 (Jan. 25, 2007) (modification), for records maintained in JABS. This notice mitigates the risk that the individual will not know why the information is being collected or how the information will be used. No other notice is required to be provided because the information in this system is collected during law enforcement activities and it is not practicable for any other notice to be given during these activities. 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 CFR 16.131).

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: Feb. 28, 2011 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:	
X	A security risk assessment has been conducted.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Current certification and accreditation packages identify data security controls; monthly vulnerability scans are conducted to identify whether there are any weaknesses which can be exploited for unauthorized intrusion.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: (1) Monthly vulnerability scans are conducted to identify whether there are any weaknesses which can be exploited for unauthorized intrusion. (2) A contingency planning (CP) exercise and incident response (IR) exercise was conducted in 2009 in which the JABS Program participated. The JABS Program Office maintains a Business Continuity and Contingency Plan (BCCP) that documents the strategies, personnel, procedures, and resources that will be used to minimize disruptions of JABS.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Monthly vulnerability scans are conducted to identify whether there are any weaknesses which can be exploited for unauthorized intrusion. As described above, the JABS Program participated in the DOJ Contingency Planning Exercise and Incident Response exercise in 2009 and maintains a BCCP and keeps certification and accreditation packages current.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

The system has role-based access controls. Access to specific data is restricted by user classification. The detail level of the information available is limited by the user classification. The system retains the user's role and adjusts the functionality as appropriate to that role. User roles are clearly and specifically defined providing for the various levels of access. The system has database auditing. The system is fully Certified and Accredited (C&A) according to generally accepted guidelines for C&A of DOJ systems and re-accredited every 3 years. JABS runs monthly vulnerability assessment scans on the system and manages any found vulnerabilities. Additional information can be found in sections: 6.1, 2.3, and 3.5.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: Justice/DOJ-005 (Nationwide Joint Automated Booking System), 71 Fed. Reg. 52821 (Sept. 7, 2006), 72 Fed. Reg. 3410 (Jan. 25, 2007) (modification - one new routine use); Justice/DOJ-002 (DOJ Computer Systems Activity and Access Records), 64 Fed. Reg. 73585 (Dec. 30, 1999), 66 Fed. Reg. 8425 (Jan. 31, 2001) (modification - new routine use), 72 Fed. Reg. 3410 (Jan. 25, 2007) (modification - new routine use)
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

The query tool is used to retrieve information by any database field. Users who receive extracts of JABS information retrieve information by any database field in the extract. Rap sheets are retrieved by submitting a suspect’s fingerprints to JABS.

Appendix A: Information collected, maintained, used, or disseminated by the system

Below is a list of data that may be collected as part of the JABS booking process. Note that not every data element is collected for every booking; however, fingerprints, booking date, booking time, JABS transaction ID, FBI number, and ORI code are required for each booking.

General Data

1. Fingerprints
2. Booking Date
3. Booking Time
4. JABS Transaction ID
5. FBI Number

Arrest Data

1. Official Collecting Data
2. Arresting Agent
3. Arresting Agent's phone number
4. Arresting Agency ORI Code
5. Arresting Agency
6. Charges
7. Warrants
8. Jurisdiction

Arrestee Data

1. Name
2. Gender
3. Height, Weight
4. Social Security Number
5. Eye, Hair Color
6. Ethnicity
7. Marital Status
8. Minor or Adult
9. Text-based Description of Scars, Marks, and Tattoos
10. Missing Limbs or Fingers
11. Phone Number(s), Address(es)
12. Vehicle Information: Make, Model, Color, VIN, Year, License Plates, State
13. Facial Features
14. Documentation for Foreign Residents (i.e. Visa Type, Nation, and #)
15. Citizenship, Date of Birth
16. Associates’ Names
17. Prescription Drugs

Extracts

Four Law Enforcement organizations receive extracts of JABS data on set intervals: The four extracts are subsets deemed necessary by the requesting organization to assist in their investigations and/or prisoner management, but are not used for booking. In some cases, the data requested is not specific to a prisoner, but rather reference tables that are used to interpret data from booking packages. The words “types,” “codes,” “classes,” and “categories” indicate this class of data. The four extracts contain the following information:

ACTIC (Arizona Counter Terrorism Information Center) and Pinellas County (Fla.)

1. Front photo/mug shot
2. Date of photo
3. Arrestee's name
4. Arrestee's date of birth
5. Arrestee's Gender
6. Arrestee's height
7. Arrestee's weight
8. Arrestee's eye color
9. Arrestee's hair color
10. Arresting Agency ORI Code
11. Arresting ORI
12. Arresting agent's name
13. Arresting agent's phone number
14. Arrestee's FBI #

DEA

1. Agencies
2. Agency_Roles
3. AMP_Codes
4. Arrest_Types
5. Associate_Types
6. Booking_Types
7. Countries
8. Documentation
9. Ethnicity
10. Eye_Colors
11. Facial Attributes
12. Fingers
13. Gender
14. Hair Colors
15. Image_Category
16. Image_Types
17. Jurisdictions
18. Location_Types
19. Marital_Stat_Types
20. Poses
21. Race_Types

22. SMT_Keywords
23. States
24. Tattoo_Classes
25. Tattoo_Colors
26. Tattoo_Subclasses
27. Tattoos

OCDETF (Organized Crime Drug Enforcement Task Force)

1. Agencies
2. Agency_Roles
3. AMP_Codes
4. Arrest_Types
5. Associate_Types
6. Booking_Types
7. Countries
8. Document_Types
9. Ethnicity_Types
10. Eye_Colors
11. Facial_Attributes
12. Fingers
13. Gender_Types
14. Hair_Colors
15. ID_Char_Types
16. Image_Categories
17. Image_Types
18. Jurisdictions
19. Location_Types
20. Marital_Stat_Types
21. Poses
22. Race_Types
23. SMT_Keywords
24. States
25. Tattoo_Classes
26. Tattoo_Colors
27. Tattoo_Subclasses
28. Tattoos
29. Agency_locations