

Nationwide JABS

Department of Justice Joint Automated Booking System

Privacy Impact Assessment



Version 1.4

January 21, 2002

LIMITED OFFICIAL USE

Prepared for the:
JABS Program Management Office
United States Department of Justice
901 E Street, NW, Suite 510
Washington, DC 20530

This page intentionally left blank

Nationwide JABS

Department of Justice Joint Automated Booking System

Abstract

The *Joint Automated Booking System* (JABS) Privacy Impact Assessment (PIA) document identifies and addresses the privacy impact issues and processes. Contained within are privacy issues for JABS which have relevance for both the Client Workstation and Server Site environments.

The Privacy Act of 1974, as Amended (5 United States Code 552a) and the Computer Matching and Privacy Act of 1988 (Public Law 100-503) afford individuals the right to privacy in records maintained and used by Federal agencies. The Department of Justice (DOJ) is responsible for ensuring the privacy, confidentiality, integrity, and availability of individuals, applicants, and employee information. The PIA is a process used to evaluate privacy in information systems.

LIMITED OFFICIAL USE

This page intentionally left blank

Table of Contents

Abstract

Document Change History Page	iii
Section 1.0: Introduction	1
1.1 Background	1
1.2 Purpose of Document	2
1.3 Scope	2
1.4 Definition of Terms	2
1.5 References	2
Section 2.0: System Description and Type of Records	3
2.1 Data in the System	3
2.2 Data Disposition	5
Section 3.0: Volume of Records	7
3.1 Current Volume of Records Processed Through JABS	7
3.2 JABS Capacity for Processing Records	7
Section 4.0: Person and Organizational Access	9
4.1 Access to the Data	9
4.2 How Access is Determined and Controlled	9
4.3 Indirect User Access to Data	9
4.4 Other Systems Access to Data	9
Section 5.0: Purpose of System Data	12
5.1 Extent to Which System Data is Used	12
5.2 Extent to Which System Data is Required	12
5.3 Extent to Which System Data is Analyzed and Assessed	12
Section 6.0: Sources of Data	14
6.1 Indirect User Data Input from the Offender	14
6.2 FBI IAFIS Data Source	14
Section 7.0: Processes for Verifying Data Accuracy	16
7.1 Indirect User Verification	16
7.2 FBI IAFIS Verification	16

Nationwide JABS

Department of Justice Joint Automated Booking System

Section 8.0: Assessment 18

Appendix A - List of Acronyms A-1

Appendix B - Request for Records Disposition Authority B-1

LIMITED OFFICIAL USE

Nationwide JABS

Department of Justice Joint Automated Booking System

Document Change History Page

Date	Ver. #	Description of Change	Author
12-21-01	Version 1.4	Updated the JABS PIA with significant changes from the Version 1.4 software enhancements.	M. Greggs

This page intentionally left blank

Nationwide JABS

Department of Justice Joint Automated Booking System

Section 1.0: Introduction

1.1 Background

Joint Automated Booking Services (JABS) is an information sharing system and 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 the automated booking stations and booking systems of Department of Justice (DOJ) components and maintains a shared repository that can be accessed by all participating agencies. 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 agencies as the situation, personal data, or geographic location changes. JABS also provides agencies with the connectivity needed to submit fingerprints to IAFIS electronically and receive the resulting fingerprint and offender identification and criminal history findings. All communications are planned to be provided by the Justice Consolidated Network (JCN) and FBI Criminal Justice Information Services (CJIS).

The initial subscribers of JABS are the five DOJ components that book offenders: the Bureau of Prisons (BOP), Drug Enforcement Administration (DEA), FBI, Immigration and Naturalization Service (INS), and U.S. Marshals Service (USMS). Other agencies that originate booking data (federal, state, and local) are expected to become subscribers in the future. JABS will also have users who do not originate JABS data, but require occasional access to such data, for example, the Bureau of Justice Statistics, Executive Office of United States Attorneys, National Drug Intelligence Center, and Agency Headquarter Organizations.

The operational workflow of JABS begins with an arrest at a DOJ law enforcement agency. The offender is booked using an automated booking station designed for the particular agency's unique business practices and within its existing or planned technology infrastructure. At the discretion of a component, a booking station may submit booking data to JABS directly or through its agency's central booking system. The booking package will be made up of standard data elements and submitted to JABS via e-mail transported by the JCN. JABS validates each booking package and forwards digital fingerprints to FBI's IAFIS for identification. Communication with IAFIS is via connection at the JDC-W with the FBI's CJIS network. Identifying information returned by IAFIS is forwarded to the submitting party via a JCN-transmitted e-mail message.

A record of the transaction is stored in the JABS database. Subsequent processing agencies, such as USMS and BOP, access JABS to capture the online booking package and FBI response in

LIMITED OFFICIAL USE

Nationwide JABS

Department of Justice Joint Automated Booking System

order to create their own agency-unique database records on the offender. Users access the JABS database through the browser capabilities of their personal computers (PCs) or booking stations and JCN connectivity. An authorized user can enter known offender characteristics, such as name, birthday, Social Security Number (SSN), and vehicle license number to search for matching records in the JABS database. The user can view and print the offender summary, personal history report, booking history, and photos.

1.2 Purpose of Document

This document shall serve to determine if an updated Systems of Records Notice (SORN) is needed for Version 1.4 of JABS. The original SORN for Nationwide JABS was published April 2001. The SORN defines who, what, when, where, and why a file exists in a government agency.

1.3 Scope

The scope of this document adheres to the guidelines for reviewing and assessing privacy issues with regards to the JABS. The JABS Privacy Impact Assessment (PIA) describes the offender's privacy issues for both the Client Workstation and Server Site environments.

1.4 Definition of Terms

See Appendix A for a list of acronyms of words found within this document.

1.5 References

- a. DOJ 2880.1A, Information Resources Management
- b. US Department of Justice, DOJ-TP-002, *DOJ Information Technology Systems Security Certification and Accreditation Standard and Implementation Guidelines*, November 10, 1999.
- c. US Department of Justice, *DOJ Systems Development Life Cycle Manual*.

LIMITED OFFICIAL USE

Section 2.0: System Description and Type of Records

The JABS is an information sharing system and a conduit for sending standard booking data directly to the Federal Bureau of Investigation's IAFIS. JABS receives common offender data elements (biographical data, fingerprints, and photographs) from the automated booking stations and booking systems of DOJ components and maintains a shared repository that can be accessed by all participating agencies. 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 agencies as the situation, personal data, or geographic location changes. JABS also provides agencies with the connectivity needed to submit fingerprints to IAFIS electronically and receive the resulting fingerprint and offender identification and criminal history findings. All communications are planned to be provided by the JCN and FBI CJIS.

2.1 Data in the System

The JABS captures and transmits the following type of records:

- **Booking data:**

The data files include the following sensitive information:

- ◆ Offender's Name (First, MI, Last, & Suffix)
- ◆ Social Security Number (SSN)
- ◆ Place of Birth (POB)
- ◆ Date of Birth (DOB)
- ◆ Gender
- ◆ Race
- ◆ Height
- ◆ Weight
- ◆ Eye Color
- ◆ Hair Color
- ◆ Residential Address (Street, City, State, Zip Code, & Country)
- ◆ Offender Occupation or position
- ◆ Employer and Address
- ◆ Aliases or Maiden Name(s)
- ◆ Identifying Scars, Marks, and Tattoos
- ◆ Date of Arrest
- ◆ Date of Offense
- ◆ Action to be Taken
- ◆ Originating Agency Case Number
- ◆ Offender's Fingerprints

LIMITED OFFICIAL USE

Nationwide JABS

Department of Justice Joint Automated Booking System

- **IAFIS Response Data:**

Once IAFIS has received the information, it will search the Criminal Master fingerprint file, and Fingerprint Image Comparison (FIC) operators in Clarksburg, WVA will verify candidates. Every incoming offender transaction will generate a response. For all positively identified candidates, the Computerized Criminal History (CCH) text data (also called the Record of Arrest Printed (RAP) sheet) will be formulated into a file and transmitted back to JABS along with the response. Non-ident responses will state that no candidates were found. The response for which a candidate was uncovered will include the FBI Number of the candidate, and the candidate's criminal history in a text file.

The criminal history data will consist of multiple segments. Besides the identification segment, which contains demographics fields, three other segment types may be present that each refer to an action that has taken place in the life of the criminal subject. Depending upon the subject's criminal activity, many segments can be included. Contents of segment types are described below:

- ◆ **Identification Segment**

Includes the composite of all criminal arrest fields submitted on criminal arrest transactions (i.e., FD-249 (Federal Document 249) form arrest cards). Fields include: FBI Number (assigned uniquely for each subject), State Identification number(s), (SID)s (assigned by each state in which the subject was arrested), SSN (if known), all reported names and aliases, race, gender, POB, DOB, height, weight, eye color, hair color, and Scars Marks and Tattoos (SMT). Of prime importance, if the subject is currently wanted by any jurisdiction, the RAP sheet will specify this information.

- ◆ **Arrest Segment**

Contains details of a given arrest event. This information specifies date of arrest, the arresting agency and location of the arrest, Original Case Arrest (OCA) (arrest identification number assigned by the arresting agency) and all charges brought against subject.

- ◆ **Court Segment**

For every arrest segment, the subject's RAP sheet should optimally include a corresponding court segment, which will include the subject's disposition data. The segment fields will include date and location of the disposition, as well as sentencing information.

- ◆ **Custody Segment**

In the event that the subject was sentenced to confinement, a custody segment will

LIMITED OFFICIAL USE

Nationwide JABS

Department of Justice Joint Automated Booking System

be included in the RAP sheet that will specify the penal institution of confinement and the extent of confinement.

2.2 Data Disposition

The JABS has established guidelines for the storage, retention, destruction, and disposal of system data as appropriate. See Appendix B - Request for Records Disposition Authority (a paper-copy from Bernie Bergland's office), for information as to how long information is retained within the system.

LIMITED OFFICIAL USE

This page intentionally left blank

Nationwide JABS

Department of Justice Joint Automated Booking System

Section 3.0: Volume of Records

3.1 Current Volume of Records Processed Through JABS

Since the implementation and fielding of JABS Version 1 in July 2000, the system has been deployed and is in use by the DEA. Currently, there are several other DOJ components interested and planning to begin their use of JABS. The system has steadily increased to the current volume of an average of 200+ criminal records each month.

3.2 JABS Capacity for Processing Records

JABS has the capacity for processing high volumes of booking packages. Exact capacity and expected measurements for processing an arrestee and/or booking package has not been completed at this time.

LIMITED OFFICIAL USE

This page intentionally left blank

Nationwide JABS

Department of Justice Joint Automated Booking System

Section 4.0: Person and Organizational Access

From the security perspective, JABS has a Security Program Manager (SPM) with overall guidance and two types of users: Direct Users and Indirect Users. Direct users are those who login to JABS with an interactive session, to include JABS subscribers that use the web browser, system administrators, database administrators and system security officers. Indirect users submit booking packages via electronic mail through the JABS mail server but do not have interactive sessions with the JABS during the submission process. Note that JABS subscribers are considered to be direct users when they interact with the browser and indirect users when they are submitting a booking package.

4.1 Access to the Data

The following personnel will have access to the data in the JABS:

- ◆ Security Program Manager (SPM)
- ◆ Indirect User
- ◆ Direct User
- ◆ Metric Analyst (no visibility to data, but access Core JABS)
- ◆ System Administrator (SA)
- ◆ Security Administrator
- ◆ Database Administrator (DBA)
- ◆ FBI Fingerprint Examiners in Clarksburg, WV

4.2 How Access is Determined and Controlled

A user's job position and need-to-know determine the type of access to the data. The manager, SA, and SPM grant approval for system access. Access is immediately terminated when the individual no longer requires access to the system.

4.3 Indirect User Access to Data

An Indirect User has access only to the arrestee data files that he/she captured and transmitted through JABS. An Indirect User can work on the packages that he/she submitted (or was as alternative recipient for) and the returning e-mails from the IAFIS system. The Indirect User does not have access at any other level.

4.4 Other Systems Access to Data

JABS workstations transmits data records through the Core JABS and into the FBI IAFIS. Core JABS acts as a data repository and interface between JABS booking stations and IAFIS. IAFIS uses the data records to determine whether the arrestee for a given package is found within the FBI Criminal Master File (CMF).

LIMITED OFFICIAL USE

This page intentionally left blank

Nationwide JABS

Department of Justice Joint Automated Booking System

Section 5.0: Purpose of System Data

JABS automates the collection and transmission of identification and biographical data, including fingerprints and photographs of offenders.

The JABS Program goals are to:

1. Automate the collection and transmission of identification and biographical data, including fingerprints and photographs of offenders.
2. Provide an automated conduit for federal criminal justice agencies to IAFIS.
3. Support the automation of federal booking processes.
4. Reduce process and data redundancies in arrest bookings through data sharing.
5. Reduce the time required for positive identification and processing of offenders.
6. Enable law enforcement organizations to track offenders from booking through disposition.
7. Enable law enforcement organizations to share and exchange booking information.

5.1 Extent to Which System Data is Used

The functionality of JABS (from the data it captures) has the distinct capability of assisting federal agencies to identify previous criminal offenses, identify individuals subject to the criminal justice process, or conduct criminal or intelligence investigations. For an arrestee with positive match within IAFIS, JABS can provide to the DOJ component the RAP Sheet for this individual.

5.2 Extent to Which System Data is Required

The metrics program for JABS does not require by statute, or need that system data be maintained or used solely as statistical reporting. JABS will contain metric capturing functionality, but no individual arrestee data will be used. Metrics for the JABS will be used to benchmark performance requirements and to allow for system performance monitoring.

5.3 Extent to Which System Data is Analyzed and Assessed

The Joint Automated Booking System's primary objective is to provide the DOJ Organizations (i.e., Indirect Users) with a rapid criminal history check and capability to submit fingerprints as part of the organization's background investigation. Based on IAFIS and core JABS output, the Indirect User will be able to quickly analyze any adverse data and determine subsequent actions.

LIMITED OFFICIAL USE

This page intentionally left blank

Nationwide JABS

Department of Justice Joint Automated Booking System

Section 6.0: Sources of Data

JABS has two sources of data used in the background investigation of an arrestee package. Initially, the arrestee package is collected and assimilated at the JABS workstation. JABS collects an arrestee's biographical information directly from the offender at the agencies workstation. Individual fingerprints are gathered from offender by the use of live scan. This data is directed to the FBI IAFIS system for a match/search against the FBI's CMF. The second data source, the CMF, provides RAP sheets when a positive identification is made for an arrestee booking package.

6.1 Indirect User Data Input from the Offender

Information used to create the booking Package and entered into the JABS is collected from the offender at the time of apprehension.

6.2 FBI IAFIS Data Source

Information contained in the RAP sheet is obtained from multiple organizations in the country's criminal justice system. Arrest text information is obtained from FD-249 arrest cards and live-scan operation data originally collected at law enforcement offices. Court segment data is obtained from disposition reports created at the court and originating at time of trial completion. Custody data is created at the prison at time of confinement. IAFIS normally receives the criminal history data indirectly from the 50 state identification bureaus and not from the organizations who actually developed the criminal history information.

LIMITED OFFICIAL USE

This page intentionally left blank

Section 7.0: Processes for Verifying Data Accuracy

7.1 Indirect User Verification

JABS provides the interface for the Indirect User to capture all the mandatory (and non-mandatory) information necessary to process an arrestee's booking package through the FBI's IAFIS system. The Indirect User is responsible for verifying that the information entered is deemed valid and accurate. This individual works with the arrestee to capture his/her biographical information and fingerprints. Prior to submitting the package, the JABS software will verify that all mandatory information is included within the record.

7.2 FBI IAFIS Verification

FBI maintains the IAFIS system that contains the 41+ million records in the CMF. The integrity of the CMF is highly guarded and maintained by the staff of the FBI. Individual subject records are totally checked by FBI operators in Clarksburg, West Virginia before including new information into an existing record. Whenever an arrest transaction is initially received by IAFIS, the fingerprint images are checked by an FBI operator for suitable quality and potential finger transposition error before that transaction is searched. The transaction can then undergo a name search and probably a fingerprint search to check for criminal candidates. The FBI CJIS Division has employed a group of fingerprint experts in a FIC group who compare all fingerprints of incoming transactions with CMF candidates. For all candidates found, two different FIC operators independently verify each candidate. The same procedure applies to arrestee searches. When an arrestee package is received and the biographical data and fingerprints are used to identify a candidate within the CMF, human verification of two FIC operators are performed on the subject's results. This process adds an additional layer of data accuracy and verification to the JABS process.

This page intentionally left blank

Nationwide JABS

Department of Justice Joint Automated Booking System

Section 8.0: Assessment

As stated in Section 1.2 of this document, the purpose of the PIA is to determine if an “updated” System of Records Notice is needed for the JABS Version 1.4. This section provides the findings and assessment by the Program Management Office (PMO) with regards to safeguarding the offender’s personal privacy data. Specifically, this PIA assesses and ensures that JABS protects the privacy of individuals by:

- ◆ Complying with the provisions of the Privacy Act
- ◆ Safeguarding individuals against invasion of personal privacy
- ◆ Ensuring that information captured in JABS is accurate, relevant, timely, and complete
- ◆ Providing protection for the offender’s Privacy Act records

After completing the PIA, the PMO has discerned the following evaluation of the privacy impact for the JABS:

- ◆ JABS Version 1.4 requirements contain no changes that offset the current Privacy Act conditions
- ◆ The JABS program published a SORN declaration in the Federal Registry, Vol 66, No. 78; Monday, April 23, 2001 for Version 1.0
- ◆ JABS workstations are covered by existing privacy notices already in place in the user organizations.

In November 2000 through the evaluation and assessment of the privacy impacts for the JABS, it was determined that the JABS Version 1.0 was subject to a SORN, subsequently published. Pursuant to the regulations detailed in the OMB Circular No. A-130 (November 30, 2000) Appendix I, 5 U.S.C. 552a, Privacy Act of 1974, and DOJ 2640.1, Privacy Act Security Regulations for Systems of Records, dated February 8, 1977, a SORN is required under the following conditions:

- ◆ “The Privacy Act applies when the Federal Government has in place a “system of records”, which is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

LIMITED OFFICIAL USE

Nationwide JABS

Department of Justice Joint Automated Booking System

However, because the requirements for Version 1.4 does not exceed the boundaries of the current SORN, the PMO believes the previously published SORN is still in effect and accurately reflects the capture, storage, processing, and control of the JABS data.

LIMITED OFFICIAL USE

Appendix A

List of Acronyms

CCH	Computerize Criminal History
CJIS	FBI Criminal Justice Identification System
CMF	Criminal Master File
DAC	Discretionary Access Control
DBA	Database Administrator
DES	Data Encryption Standard
DOB	Date of Birth
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FD-249	Federal Document 249
FIC	Fingerprint Image Comparison
FIPS	Federal Information Processing Standard
IAFIS	Integrated Automated Fingerprint Identification System
JABS	Joint Automated Booking System
JCN	Justice Consolidated Network
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OCA	Original Case Arrest
OMB	Office of Management and Budget
ORI Code	Origination Code
PIA	Privacy Impact Assessment
PMO	Program Management Office
POB	Place of Birth
RAP	Record of Arrest Printed
SA	System Administrator
SID	State Identification Number
SMT	Scars, Marks, and Tattoos
SORN	System of Records Notice
SPM	Security Program Manager
SSN	Social Security Number

LIMITED OFFICIAL USE

This page intentionally left blank

Appendix B
Request for Records Disposition Authority

(Paper attachment to follow this title page)

LIMITED OFFICIAL USE

