Civil Applicant System

Department of Justice Civil Applicant System

Privacy Impact Assessment

Version 2

September 28, 2001

LIMITED OFFICIAL USE

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

Abstract

The *Civil Applicant System* (CAS) Privacy Impact Assessment (PIA) document identifies and addresses the privacy impact issues and processes. Contained within are privacy issues for CAS 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 Privacy Impact Assessment (PIA) is a process used to evaluate privacy in information systems.

Table of Contents

List of Tables

Document Change History Page

Date	Ver. #	Description of Change	Author

Section 1.0: Introduction

1.1 Background

The Department of Justice (DOJ) has developed the Civil Applicant System (CAS) which enables DOJ's Components and other authorized and participating federal agencies to electronically capture civil applicant fingerprints and biographical data and to transmit the data to the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS) as part of their background investigations of potential DOJ employees, political appointees, and contractor personnel.

1.2 Purpose of Document

This document shall serve to determine if a Systems of Records Notice (SORN) is needed for the CAS. 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 CAS. The CAS Privacy Impact Assessment (PIA) describes the applicant 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. US Department of Justice, CJIS-RS-0010 (V7), DOJ Criminal Justice Identification System (CJIS) *Electronic Fingerprint Transmission Specification*, January 29, 1999.

b. US Department of Justice, *DOJ Certification and Accreditation Program Guidance*, DRAFT, July 2, 2001.

c. US Department of Justice, DOJ-TP-002, *DOJ Information Technology Systems Security Certification and Accreditation Standard and Implementation Guidelines*, November 10, 1999.

d. US Department of Justice, *DOJ Systems Development Life Cycle Manual*.

e. US Department of Justice, *Information Resource Management Order*.

Section 2.0: System Description and Type of Records

The Civil Applicant System (CAS) electronically captures and documents the fingerprints and biographical data of civil applicants for Department of Justice (DOJ) components (or other participating Federal agencies), political appointees, and contracting staff. The CAS software then transmits this information to the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprinting Investigation (IAFIS) as part of their background investigations.

2.1 Data in the System

The CAS captures and transmits the following type of records:

- **Applicant data:**

The data files include the following sensitive information:

- Applicant'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
- Complete Residential Address (Street, City, State, Zip Code, & Country)
- Employing Government Agency
- Address of Government Agency
- Applicant Occupation or position
- Aliases or Maiden Name(s)
- Identifying Scars, Marks, and Tattoos
- Applicant's Fingerprints

- **Employee Data:**

The CAS records used in the transmission of applicant information contains the employee's (i.e., the End User) e-mail address, ORI (origination) code, and name.

- **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 civil applicant transaction will generate a response. For all positively identified candidates, the Computerized Criminal History (CCH) text data (also called the RAP sheet) will be formulated into a file and transmitted back to CAS 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 Record of Arrest Printed (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 be included in the RAP sheet that will specify the penal institution of confinement and the extent of confinement.

2.2 Data Disposition

The CAS has established guidelines for the storage, retention, destruction, and disposal of system data as appropriate. See Table 2-1 for information as to how long information is retained within the system.

Table 2-1. Record Disposition Schedule

Data Storage Locations	Type of Data Stored	Retention Policy
USER e-mail box (Exchange) – *Note:* **Three** types of messages: 1) those received from the submitter; 2) status messages sent from CAS to the submitter; and 3) those received from the IAFIS e-mail box.	– applicant bio & fingerprints – RAP sheet, FBI name, FBI number – IAFIS response type (ident/non-ident, success/error) – transaction status (error/complete/waiting for IAFIS)	Delete all data immediately upon processing to the next stage (e.g., transmission to the IAFIS e-mail box or to the submitter).
IAFIS e-mail box (Exchange) – *Note:* **Two types of messages:** 1) those received from User e-mail box, and 2) those received from IAFIS	– applicant bio & fingerprints – RAP sheet, FBI name, FBI number – IAFIS response type (ident/non-ident, success/error)	– Message Type 1 – Delete immediately upon sending to IAFIS – Message Type 2 – Delete "success" responses; "error" responses to be deleted after 5 days; copy error message in response to database
File System (jdata)	– applicant bio & fingerprints – RAP sheet, FBI name, FBI number – IAFIS response type (ident/non-ident, success/error)	Delete all data after receiving IAFIS response (24 hours or less).
Database – *Note:* The database contains info required for security audit trails.	– IAFIS response type (ident/non-ident, success/error) – transaction metrics (success/error, error message (if any), processing time, submitting user) – transaction status (error/complete/waiting for IAFIS)	Delete data that is 90 days or older every month after collecting system metrics.
Application Logs	– transaction status (error/complete/waiting for IAFIS) – data pertaining to the functioning of the system/application	Delete all data weekly.

Data Storage Locations	Type of Data Stored	Retention Policy
Backups		Do NOT back up the following data types: – applicant bio & fingerprints – RAP sheet, FBI name, FBI number – IAFIS response type (except in Database) DO back up the following data storage locations: – Database – Application Logs

Section 3.0: Volume of Records

3.1 Current Volume of Records Processed Through CAS

Since the implementation and fielding of CAS in November 2000, the system has been deployed to three DOJ organizations. Currently, there are several other DOJ components and federal agencies interested in using CAS. The system initially processed approximately 100+ applicant packages each month, but has steadily increased to the current volume of an average of 500+ records each month.

3.2 CAS Capacity for Processing Records

CAS has the capacity for processing high volumes of civil applicant packages. Exact capacity and expected measurements for processing applicant packages has not been completed at this time.

Section 4.0: Person and Organizational Access

From the security perspective, CAS will have a Security Program Manager (SPM) with overall guidance and two types of users: End Users and Privileged Users. Privileged Users are those who login to the CAS server site with an interactive session, to include system administrators, metric analysts, and security administrators. End Users submit applicant packages via electronic mail from the client application through the CAS server.

4.1 Access to the Data

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

- Security Program Manager (SPM)
- End User
- Metric Analyst (no visibility to data, but access Core JABS/CAS)
- 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, System Administrator (SA), and SPM grant approval for system access. Access is immediately terminated when the individual no longer requires access to the system.

4.3 End User Access to Data

An End User has access only to the applicant data files that he/she captured and transmitted through CAS. An End 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 End User does not have access at any other level.

4.4 Other Systems Access to Data

CAS transmits data records through the Core JABS and into the FBI IAFIS. However, neither Core JABS nor IAFIS share CAS data with other systems. Core JABS acts only as the interface between CAS and IAFIS. IAFIS uses the data records to determine whether the applicant for a given package is found within the FBI Criminal Master File.

Section 5.0: Purpose of System Data

CAS is designed to capture and transmit applicant biographical and fingerprint information of individuals applying for civil positions within the Federal Government. The data captured is retained for a minimum period of time until a response from IAFIS is received. Afterwards, the data is purged from the system and is unavailable for access.

5.1 Extent to Which System Data is Used

The functionality of CAS (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 applicant with positive match within IAFIS, CAS will provide to the DOJ component the RAP Sheet for this individual.

5.2 Extent to Which System Data is Required

The metrics program for CAS does not require by statute or need that system data be maintained or used solely as statistical reporting. CAS will contain metric capturing functionality, but no applicant data or employee data will be used. Metrics for the CAS 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 Civil Applicant System's primary objective is to provide the End User Organization with a rapid criminal history check on fingerprints as part of the organization's normal clearance process. CAS functionality does not determine suitability or eligibility for employment access to classified information, or for promotion. Based on IAFIS and CAS output, the End User (or organization) will be able to quickly analyze any adverse data and determine employment options.

Section 6.0: Sources of Data

CAS has two sources of data used in the background investigation of an applicant package. Initially, the applicant package is collected and assimilated at the CAS workstation. CAS collects an applicant's biographical information directly from the civil application form. Individual fingerprints are gathered from fingerprint cards or by live scan. This data is directed to the FBI IAFIS system for a match/search against the FBI's Criminal Master File (CMF). The second data source, the CMF, provides RAP sheets when a positive identification is made for a civil applicant package.

6.1 End User Data Input from the Applicant

Information used to create the Applicant Package and entered into the CAS is collected from the individual at the time of applying for a civil service position.

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 police stations. 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.

Section 7.0: Processes for Verifying Data Accuracy

7.1 End User Verification

CAS provides the interface for the End User to capture all the mandatory (and non-mandatory) information necessary to process an applicant package through the FBI's IAFIS system. The End User is responsible for verifying that the information entered is deemed valid and accurate. This individual works with the applicant to capture his/her biographical information and fingerprints. Prior to submitting the package, the CAS 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 40+ 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 WVA 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 Fingerprint Image Comparison (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 applicant searches. When an applicant 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 CAS process.

Section 8.0: Assessment

As stated in Section 1.2 of this document, the purpose of the PIA is to determine if a SORN is needed for the Civil Applicant System. This section provides the findings and assessment by the Program Management Office (PMO) with regards to safeguarding the applicant's personal privacy data. Specifically, this PIA assesses and ensures that CAS 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 CAS is accurate, relevant, timely, and complete
- Providing protection for the applicant's Privacy Act records

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

- CAS automates processes that are currently performed manually.
- Privacy data is not stored by CAS.
- CAS is covered by existing privacy notices already in place in the user organizations.

Through the evaluation and assessment of the Privacy Impacts for the CAS Version 2, it has been determined that this systems is not subject to a SORN. 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."

Because the CAS is not a "systems of records" under which a group of records are controlled by an agency, nor a system from which information is retrieved. Therefore, the CAS does not fall within the specified criteria as outlined in the above paragraphs.

Appendix A
List of Acronyms

CAS	Civil Applicant System
CCH	Computerize Criminal History
CJIS	FBI Criminal Justice Identification System
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 Standards
IAFIS	Integrated Automated Fingerprint Identification System
JABS	Joint Automated Booking System
NACI	National Agency Check and Inquiries
NIST	National Institute of Standards and Technology
OCA	Original Case Arrest
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