Fingerprint Transaction System (FTS)

Privacy Impact Assessment

1. IT System or Electronic Information Collection Identification

a. Who is completing the initial screening assessment?

Program Analyst, FISD/CSB.

b. Who is the IT system or electronic information collection owner?

Deputy Associate Director for Services, FISD.

c. What is the IT system or electronic information collection name?

Fingerprint Transaction System (FTS).

d. Does the activity represent a new or significantly modified IT system or information collection?

No.

e. Is this an IT system or project or an electronic information collection?

IT system or project.

f. What is the Unique Project Identifier (UPI)?

027-00-01-02-02-1045-00.

g. Will this IT system or electronic information collection use web technology?

No.

h. What is the purpose of the IT system or electronic information collection and why is the information being collected?

Used in the federal investigative process to conduct fingerprint checks.

i. What is the IT system or electronic information collection status?

Operational.

j. Is the IT system or electronic information collection operated by OPM staff, contractor staff, or a combination of OPM and contractor staff?

Combination of OPM staff and contractor staff.
USIS, OCIO-NMG Contractors.

k. Where is the IT system or electronic information collection physically located?

Pennsylvania.

2. Initial Screening Assessment

a. Is an OMB mandated PIA required for this IT system or electronic information collection?

Yes.

b. Does the system or electronic information collection contain or collect any Personally Identifiable Information (PII)?

Yes.

c. Is this an IT system that collects PII on members of the public?

Yes.
Privacy information collected on applicants. Information also collected for regulatory purposes.

d. Is this an electronic information collection that collects PII on members of the public?

Yes.

e. Is this an electronic information collection that collects PII on Federal employees?

Yes.

3. The PIA

3.1. Nature and Source of Information to Be Collected

a. What is the nature of the information to be collected?

Biometric and other personal identifiers.

b. What is the source of the information?

Directly from the person to whom the information pertains; from other people; other sources such as databases, web sites, etc.

3.2. Reason for Collection of Information

a. Why is the information being collected?

The investigations conducted by OPM include verification/confirmation of subject provided information to determine suitability for a position with the government and/or for a security clearance,
and to verify identity of participants through fingerprints.

b. Is there legal authority for collecting the information?

Yes.
Executive order 10450; Executive Order 10865; Executive Order 12333; Executive Order 12356; Section 3301 & 9101 of Title 5; Sections 2165 & 2201 of Title 42; Sections 781 & 887 of Title 50; Part 5, 732 & 736 of Title 5.

3.3. Intended Use of the Collected Information

a. What is the intended use of the information?

The investigations conducted by OPM include verification/confirmation of subject provided information to determine suitability for a position with the government and/or for a security clearance,
and to verify of participants through fingerprints.

b. For major IT investments as defined in OMB Circular A-11, a high-level data flow diagram must be prepared?

Yes.

3.4. Purpose and Identification of Information to Be Shared

a. Does the system share Personally Identifiable Information (PII) in any form?

Yes.
Within OPM.
FTS shares this information with PIPS to upload cases and results, that include subject identifiers.
With other Federal agencies.
All of the subject's personal identifiers (Name, DOB, POB, SSN) plus fingerprint images are submitted to the FBI-CJIS through FTS.

b. Who will have access to the PII on the system?

Users, Administrators, Developers, and Contractors.

c. Is information part of a computer matching program?

No.

3.5. Opportunities Individuals Have to Decline to Provide Information or to Consent to Particular Uses of the Information

a. Is providing information voluntary?

Yes.

b. Are individuals informed about required or authorized uses of the information?

Yes.
Privacy Act Statement.

c. Will other uses be made of the information than those required or authorized?

No.

3.6. Security of Information

a. Has the system been authorized to process information?

Yes.

b. Is an annual review of the IT system or electronic information collection conducted as required by the Federal Information Security Management Act (FISMA)?

Yes.

c. Are security controls annually tested as required by FISMA?

Yes.

d. Are contingency plans tested annually as required by FISMA?

Yes.

e. Have personnel using the system been trained and made aware of their responsibilities for protecting the PII being collected and maintained?

Yes.

f. Are rules of behavior in place for individuals who have access to the PII on the system?

Yes.

3.7. System of Records as Required by the Privacy Act, 5 U.S.C. 552a

a. Are records on the system routinely retrieved by a personal identifier?

Yes.
The Privacy Act applies.

b. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes.
OPM/Central - 9.

c. Does the SORN address all of the required categories of information about the system?

Yes.
System name; System Classification; System location; Categories of individuals covered by the system; Categories of records; Authority of maintenance; Purpose; Routine uses of records maintained; Disclosure to consumer reporting agencies; Policies and practices for storing, retrieving, accessing, retaining, and disposing of records; System Manager and contact information; Notification procedure; Record access procedure; Contesting record procedure; Record source categories; System exempted from certain provisions of the Act.

d. Has any of the information in the SORN changed since the information was published?

No.

e. Are processes in place for periodic review of Personally Identifiable Information contained in the system to ensure that it is timely, accurate, and relevant?

Yes.
OPM/Central-9: is being revised;
Item No: 2-7 Investigations;
Disposition: 3 months – 10 years.

4. Certification

A PIA is required and the OPM Chief Privacy Officer signed the PIA on August 2, 2007.