Personnel Investigations Processing System (PIPS)

Privacy Impact Assessment

1. IT System of Electronic Collection Identification

a. Who is completing the initial screening assessment?

Chief, Support System Branch, FISD/ITP/SSB.

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

Program Manager, Information Technology Program, FISD/ITP.

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

Personnel Investigations Processing System (PIPS).

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)?

027-00-01-02-02-1040-00-315-179.

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

Yes.

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

The Personnel Investigations Processing System (PIPS) is an automated system which houses the Security/Suitability Investigations Index (SII) and is used by OPM-FISD for the automated entry, scheduling, case control and closing of background investigations.

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 contractors.

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

Washington, D.C.

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.

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?

Subject identification and background information needed to conduct security and/or suitability investigations.

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.

b. Is there legal authority for collecting the information?

Yes.
Executive order 10450, Public Law 82-298, Executive order 9397 (November 22, 1943), Law (title 18. us code, section 1001).

3.3. Intended Use of the Collected Information

a. What is the intended use of this 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.

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

Not Applicable.

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.

OCFO-OPM investigations are Revolving Fund products and services. Information must be shared in order to bill customers for these products and services.

With other Federal agencies.

Checks of other Federal agencies records (FBI, DSS, Selective Service, Military record repositories, Treasury, CIA, DHS, Dept of State, etc). In all instances, name/alias SSNs, POB are shared. Other information can be provided if needed by the agency. Federal agencies query the SII for reciprocity. Data can be shared with Federal agencies under files release policies.

With state or local governments.

Law enforcement entities and courts are contacted during the investigation. Minimal PII is shared to establish identity and conduct search.

With members of the Public.

Educational institutions, current and former employers, neighbors, co-workers, references, etc., are contacted during the investigation. Minimal PII is shared to establish identify, conduct search, verify/confirm sub-supplied information.

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.

Completion of information is voluntary. OPM may not be able to complete the investigation or complete in timely manner. Incomplete files may also affect the subject's placement in position and may also affect security clearance eligibility.

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.
General users.

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

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

Yes.

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.
Schedule Number: 3.INV;
Item No: 2-7 Investigations;
Disposition: 3 months – 10 years;
Last Job Number: N9-478-02-15.

4. Certification

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