Electronic Questionnaires for Investigating Processing (eQIP)

Privacy Impact Assessment

1. IT System or Electronic Information Collection Identification

a. Who is completing the initial screening assessment?

eQIP Project Manager, FISD/ITP/SSB/ASB.

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

Program Manager, FISD/ITP.

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

Electronic Questionnaires for Investigations Processing (eQIP).

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

Yes.

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

IT system or project;
Electronic information collection.

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?

Yes.

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

To electronically collect personnel investigative data of SF 86, SF 85P, and SF 85.

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?

OPM Staff.

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?

Personnel security investigative information.

b. What is the source of the information?

Directly from the person to whom the information pertains;
From other people.

3.2. Reason for Collection of Information

a. Why is the information being collected?

To conduct personnel security investigations to assess suitability for federal employment and access to sensitive information and to determine if eligible for security clearance.

b. Is there legal authority for collecting the information?

Yes.
Executive Orders 10450, 10865, 12333 and 12356;
US Code 42;
Code of Federal Regulations Title 5 and Title 50.

3.3. Intended Use of the Collected Information

a. What is the intended use of the information?

To conduct background investigations.

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.
e-QIP collects PII data for conducting background investigations shares with system (FISD-PIPS, OPIS).

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

Users, Administrators, 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.
After initial sign-on, user can accept or decline the terms of agreement.

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 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?

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.