ADAMS ML063200397

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment for the

Electronic Questionnaire for Investigations Processing (e-QIP)

Date: May 23, 2007

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

   e-QIP (electronic questionnaire for investigations processing) is a secure website that is owned and operated by the Office of Personnel Management (OPM). The data contained within e-QIP is sensitive but unclassified. It is designed to house all personnel investigative forms including the SF-86, "Questionnaire for National Security Positions," the SF-85P, "Questionnaire for Public Trust Positions," and the SF-85, "Questionnaire for Non-sensitive Positions." Individuals are invited into the system electronically to enter, update, and release their personal investigative data over a secure internet connection to their sponsoring agency for review, approval, and submission to our investigation provider.

2. What agency function does it support?

   e-QIP supports Personnel Security functions for the Office of Administration, Division of Facilities and Security (ADM/DFS).

3. Describe any modules or subsystems, where relevant, and their functions.

   ADM/DFS only utilizes a portion of the OPM system as detailed above. e-QIP is accessed via the OPM web portal (https://opmis.xsp.org). e-QIP is a module of the overall OPM portal and membership into this portal is by invitation only. Applicants are initiated into the system to enter their personal data to complete the required investigative paperwork listed above.

4. Points of Contact:

Project Manager	Office/Division/Branch	Telephone

Mark Lombard	**ADM/DFS**	**301-415-7739**
Business Project Manager	Office/Division/Branch	Telephone
Emily Banks	**ADM/DFS/PSB**	**301-415-0320**
Technical Project Manager	Office/Division/Branch	Telephone
Karen Cudd	**ADM/DFS/FSB**	**301-415-6554**
Executive Sponsor	Office/Division/Branch	Telephone
Timothy Hagan	**ADM/OD**	**301-415-6222**

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System ___ Modify Existing System __**X**__ Other (Explain)

The system is owned by OPM and requires approval to access the program through their secure web portal. They provide additional security layers.

b. If modifying an existing system, has a PIA been prepared before?

(1) If yes, provide the date approved and ADAMS accession number.

B. INFORMATION COLLECTED AND MAINTAINED

(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system collect information about individuals?

Yes.

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

Federal employees, Federal contractors, licensees, general public

b. What information is being maintained in the system about individuals (describe in detail)?

Info from OPM Standard Form (SF) 86, SF 85P, and SF 85, which include name, date of birth, place of birth, SSN, other names used, identifying info (hair, weight, height, eyes, sex), work/home phone numbers, citizenship, mother's maiden name, current/previous home addresses, education, employment history, name/address/phone number of references, marital status, spouse info (name, DOB, place of birth, SSN, other names used, citizenship, date/place married, separation date, address), former spouse info (name, DOB, place of birth, citizenship, date/place married, divorced/date/place, widowed/date, address), relative info (name, DOB, country of birth, citizenship, address), military history, foreign activities, foreign countries visited, medical info, police record, drug activity, alcohol use, investigations info, financial info, civil court actions.

c. Is the information being collected from the subject individuals?

Yes, the individuals complete the forms themselves.

(1) If yes, what information is being collected from the individuals?

Everything required on the forms identified above.

d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

Yes.

(1) If yes, does the information collection have OMB approval?

Yes.

(a) If yes, indicate the OMB approval number:

SF 86 - OMB No. 3206-0007
SF 85 - OMB No. 3206-0005
SF 85P - OMB No. 3206-0191

e. Is the information being collected from internal files, databases, or systems?

No.

(1) If yes, identify the files/databases/systems and the information being collected.

f. Is the information being collected from an external sources(s)?

No, only input by the individuals themselves.

(1) If yes, what is the source(s) and what type of information is being collected?

g. How will this information be verified as current, accurate, and complete?

There are numerous checks done within the e-QIP system to verify the structure of the data. The electronic document signature page is printed out, signed and certified by the individual completing the form and then sent to the individual agency. This signature page acts as the certification from the individual that the information entered electronically is current, accurate, and complete. The agency then conducts a thorough review to ensure completeness and accuracy.

h. How will the information be collected (e.g. form, data transfer)?

The information is collected via individual's data entry on the electronic forms which are then submitted to e-QIP, hiring agency accesses/reviews/verifies, then submits to OPM for investigation.

I. What legal authority authorizes the collection of this information?

Executive Orders 9397, 10450, 10577, 10865, 12333, and 12356; 5 U.S.C. 3301, 3302, and 9101; 42 U.S.C. 2165 and 2201; 50 U.S.C. 781 and 887; 5 CFR parts 5, 731, 732, 736.

j. What is the purpose for collecting this information?

The Federal Government requires background investigations and re-investigations of all Federal employees, Federal contractors, licensees, applicants, and incumbents. The Nuclear Regulatory Commission (NRC) is required to conduct national security investigations on all of its employees.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

a. What type of information will be maintained in this system (describe in detail)?

N/A

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

N/A

c. What is the purpose for collecting this information?

N/A

C. <u>USES OF SYSTEM AND INFORMATION</u>

(These questions will identify the use of the information and the accuracy of the data being used.)

1. Describe all uses made of the information.

The information is used for background investigations. NRC also uses the information during the application process for updating an existing application.

2. Is the use of the information both relevant and necessary for the purpose for which the system is designed?

Yes.

3. Who will ensure the proper use of the information?

NRC and OPM.

4. Are the data elements described in detail and documented?

Yes, with OPM.

a. If yes, what is the name of the document that contains this information and where is it located?

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will the information be *retrieved* from the system (be specific)?

Information is retrieved from e-QIP by social security number, name, or investigation request number.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

   No.

   a. If yes, explain.

      (1) What controls will be used to prevent unauthorized monitoring?

8. Describe the report(s) that will be produced from this system.

   Reports include the following:

   - How many individuals have been initiated
   - How many have not accessed the system after being invited
   - How many forms were rejected
   - How many forms are in review

   a. What are the reports used for?

      System management

   b. Who has access to these reports?

      System administrator

D. RECORDS RETENTION AND DISPOSAL

*(These questions are intended to establish whether the information contained in this system has been scheduled, or if a determination has been made that a general record schedule can be applied to the information contained in this system. Reference NUREG-0910, "*NRC Comprehensive Records Disposition Schedule*.")*

1. Has a retention schedule for this system been approved by the National Archives and Records Administration (NARA)?

   Under OPM's purview.

   a. If yes, list the disposition schedule.

2. Is there a General Records Schedule (GRS) that applies to information in this system?

Yes.

a. If yes, list the disposition schedule.

GRS 18-22a

3. If unscheduled, what are your retention requirements for the information maintained in this system? How long must the material be maintained to meet your programmatic needs?

E. ACCESS TO DATA

1. INTERNAL ACCESS

a. What organizations (offices) will have access to the information in the system?

Office of Human Resources - only has access to invite individuals to enter the system
ADM/DFS/PSB - Has access to review, approve, and submit to OPM
ADM IT Coordinators - Has access to invite users to access the system (actual user creation done by ADM/DFS/PSB after invitation and acceptance by user)

(1) For what purpose?

The system's completed forms are used to initiate background investigations. NRC also uses the information during the application process for updating an existing application.

(2) Will access be limited?

Yes, access restricted by roles.

b. Will other systems share or have access to information in the system?

No.

c. How will information be transmitted or disclosed?

The information is transmitted electronically through a secure portal within OPM. The transmission is secured with 128-bit encryption.

d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

The information is transmitted electronically through a secure portal within OPM. The transmission is secured with 128-bit encryption.

e. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes.

(1) If yes, where?

The roles are documented within e-QIP in the user roles set up area. User accounts are deleted if not entered within 90 days.

2. **EXTERNAL ACCESS**

a. Will external agencies/organizations/public share or have access to the information in this system?

Yes, but only to the individual agency's data.

(1) If yes, who.

Each agency has access to data on their employees/applicants.

b. What information will be shared/disclosed and for what purpose?

If an employee changes agencies or applies to an agency and already has an electronic form on file, the employee may grant the agency permission to begin the application process.

c. How will this information be transmitted/disclosed?

Individual agencies are not able to transmit or disclose information.

F. <u>TECHNICAL ACCESS AND SECURITY</u>

1. Describe security controls used to limit access to the system (e.g., passwords). Explain.

The Agency Administrator is responsible for creating accounts for agency employees (Users). The Agency Users are first approved access into the secure web portal by OPM officials. Then a profile is a created for each Agency User in relation to their roles and responsibilities.

A person (agency users and applicants) must be invited into the system before access is granted. An e-mail is then generated to the new user with the instructions to log in. The user then goes to the secure website and enters their social security number. Three special 'golden' questions

(NAME, DOB, POB) then appear and the user must know these answers to verify their identity. It is then user responsibility to provide and remember 'golden' questions specifically created by them. This will ensure that no one can attempt to impersonate the user on the eQIP system.

The Agency Administrator is the only individual who can reset the 'golden' questions back to the default identifiers when a user gets locked out. A lock out occurs after a user encounters three unsuccessful login attempts.

2. Will the system be accessed or operated at more than one location (site)?

   OPM controls which agencies can access the system. NRC utilizes this system at headquarters, the regions, and the TTC. The individuals may access this system wherever the internet can be accessed.

   a. If yes, how will consistent use be maintained at all sites?

      OPM determines who can access the system.

3. Which user group(s) (e.g., system administrators, project manager, etc.) have access to the system?

   Agency Administrator
   System Administrator
   Functional Administrator
   Initiators
   Reviewers
   Approvers
   Applicant/user

4. Will a record of their access to the system be captured?

   Yes.

   a. If yes, what will be collected?

      Name and role(s) held

5. Will contractors have access to the system?

   Yes.

   a. If yes, for what purpose?

      The DFS/PSB contractors initiate applicants and review/reject for incompleteness.

- Ensure that the following Federal Acquisition Regulation (FAR) clauses are referenced in all contracts/agreements/purchase order where a contractor has access to a Privacy Act system of records to ensure that the wording of the agency contracts/agreements/purchase order make the provisions of the Privacy Act binding on the contractor and his or her employees:

  - 52.224-1 Privacy Act Notification.

  - 52.224-2 Privacy Act.

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

   Under OPM's purview.

7. Are the data secured in accordance with FISMA requirements?

   OPM is responsible to comply.

   a. If yes, when was Certification and Accreditation last completed?

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL

(For Use by OIS/IRSD/RFPSB Staff)

System Name: Electronic Questionnaires for Investigations Processing (e-QIP)

Submitting Office: Office of Administration (ADM)

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

_X__ Privacy Act is applicable.

____ Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

____ Privacy Act is applicable. Currently covered under System of Records, Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

Comments:

Covered under NRC system of records NRC-39, “Personnel Security Files and Associated Records.” No modification to the system notice is required.

This system does maintain PII.

Reviewer’s Name	Title	Date
Sandra S. Northern	Privacy Program Officer	June 6, 2007

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

____ No OMB clearance is needed.

____ OMB clearance is needed.

__X__ Currently has OMB Clearance. Clearance No. SF 86 - OMB No. 3206-0007
SF 85 - OMB No. 3206-0005
SF 85P - OMB No. 3206-0191

Comments:

e-QIP (electronic questionnaire for investigations processing), a secure website that is owned and operated by the Office of Personnel Management (OPM), contains sensitive but unclassified data. It is designed to house all personnel investigative forms including the SF-86, the SF-85P, and the SF-85. Individuals enter, update, and release their personal investigative data over a secure internet connection to their sponsoring agency for review, approval, and submission to our investigation provider.

The information may be entered into the forms in eQIP from non-government respondents. Since eQIP will be used by more than 9 public respondents, it is considered a collection of information under the Paperwork Reduction Act of 1995. This collection of information has been approved under OMB Clearance numbers 3206-0007 (Form SF-86), 3206-0005 (Form SF 85), and 3206-0191 (Form SF 85P).

Reviewer’s Name	Title	Date
Christopher J. Colburn	Senior Analyst	June 12, 2007

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

___ Additional information is needed to complete assessment.

____ Needs to be scheduled.

_X__ Existing records retention and disposition schedule covers the system - no modifications needed.

____ Records retention and disposition schedule must be modified to reflect the following:

Comments:

This is an OPM system. The records maintained within this system are owned by OPM, not NRC. The retention and disposal schedule referenced in this PIA addresses the paper records printed out from this system and maintained in the Personnel Security Files.

Reviewer’s Name	Title	Date
Jeff Bartlett	Senior Records Analyst	06/12/2007

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ This IT system **does not** collect, maintain, and/or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, and/or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

___***/RA/***___ Date ___**06/15/07**___
Margaret A. Janney, Chief
Records and FOIA/Privacy Services Branch
Information and Records Services Division
Office of Information Services

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/ PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Timothy Hagan, Director, Office of Administration**

Name of System: **Electronic Questionnaire for Investigations Processing (e-QIP)**

Date RFPSB received PIA for review:
May 24, 2007

Date RFPSB completed PIA review:
June 13, 2007

Noted Issues:

Covered under NRC system of records NRC-39, "Personnel Security Files and Associated Records." No modification to the system notice is required.

This system maintains PII.

Margaret A. Janney, Chief
Records and FOIA/Privacy Services Branch
Office of Information Services

Signature/Date: ***/RA/*** ***06/15/2007***

Copies of this PIA will be provided to:

James C. Corbett, Director
Business Process Improvement and Applications Division
Office of Information Services

Kathy L. Lyons-Burke, CISSP
Senior IT Security Officer (SITSO)/Chief Information Security Officer (CISO)
Office of Information Services