Privacy Impact Assessment
for the

Electronic Questionaire for Investigations Processing (eQIP)

January 19, 2018

Contact Points

Ruth Shearer
System Owner
OCIO/NBIB IT PMO

Bruce Hunt
Acting Product Owner
NBIB/ITMO/PO

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The United States Office of Personnel Management (OPM) National Background Investigations Bureau (NBIB) conducts background investigations, reinvestigations, and continuous evaluations of individuals under consideration for, or retention of, Government employment. The purpose of Electronic Questionnaires for Investigations Processing system (e-QIP) is to provide a means to facilitate the processing of standard forms for clearance investigations. This Privacy Impact Assessment (PIA) is being conducted because e-QIP processes Personally Identifiable Information (PII) about candidates who are undergoing a background investigation and others whose information may be included in background investigation files.

Investigation Overview

The United States Office of Personnel Management (OPM) National Background Investigations Bureau (NBIB) conducts background investigations for Federal government agencies to use as the basis for suitability and security clearance determinations as required by Executive Orders and other rules and regulations. NBIB is responsible for most of the Federal government's background investigations, conducting millions of investigations each year on Federal applicants and employees, active military personnel, government contractors, and private sector employees in positions regulated by the government. In addition, NBIB has other responsibilities, including processing and providing informational reports within NBIB and to external agencies.

The background investigations consist of several major activities which involve multiple NBIB IT systems. The investigation process is initiated when a sponsoring agency requests an investigation of an identified candidate. The candidate then completes and submits various investigative forms. The information the candidate submits is reviewed and screened by the sponsoring agency's personnel security officer (or designee), who then submits the request for processing thru NBIB's Electronic Questionnaires for Investigations Processing system (e-QIP).

Interviews with the candidate and other people related to the investigation are then scheduled and assigned to an investigator or investigators by the Personnel Investigation Processing System (PIPS). The PIPS is the primary system for the processing, storing and administration of background investigations on candidates for national security, public trust and non-sensitive positions within the Federal Government. In addition other relevant information is gathered (e.g., employment, credit, criminal history), and the investigators then produce various Reports of Investigation (ROI). The ROI is then reviewed for completeness and a general case review is conducted. The case is then closed and prepared for delivery. An electronic or printed paper file is then sent to the sponsoring agency, which makes the final decision/adjudication regarding the candidate's investigation. When the sponsoring agency makes its decision regarding the candidate's investigation, it returns the decision/adjudication to the PIPS system for record keeping.

System Overview

e-QIP, the subject of this PIA, is a secure web-based automated system that was designed to facilitate the processing of standard investigative forms. e-QIP collects information directly from the applicant either via secure website or via a system-to-system connection with other agencies.

The e-QIP system allows applicants to electronically enter, update, and transmit their personal investigative data over a secure internet connection to sponsoring agencies, also known as Investigative Service Providers (ISPs) for review and approval. An ISP is a governmental organization actively involved in conducting investigations. Government agencies that request ISPs to perform background investigations can also access the e-QIP system to review the applicant's data before it is provided to any ISP. All data collected by e-QIP are sent to PIPS for processing

Section 1. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

5 C.F.R. parts 2, 5, 731, 732, 736, and 1400 establish the requirements for agencies to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions. Depending upon the purpose of the particular background investigation, NBIB is authorized to collect information under Executive Orders 9397, 10450, 10577, 10865, 12333, 12968, 13467 as amended, 13488, and 13549; 5 U.S.C. §§ 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. §§ 272b, 290a, 2519; 31 U.S.C. §§ 1537; 42 U.S.C. §§1874(b) (3), 2165, 2201, and 20132; 50 U.S.C. § 3341; Public Law 108-136; and Homeland Security Presidential Directive (HSPD) 12.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The SORN that applies to the information in e-QIP is OPM/CENTRAL 9 Personnel Investigations Records, which can be found at opm.gov/privacy.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes. The e-QIP System Security Plan (SSP), Version 1.0 November 25, 2016, was completed as part of the system's Authorization to Operate (ATO) on January 20, 2017. It was last updated to Version 3.2 on December 2017 as part of self-risk assessment.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, NARA General Records Schedule (GRS) 5.6 Security Records, item 170 and 180.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

e-QIP collects information from individuals via the forms listed below in both electronic and paper form.

Form Number	Form Name	OMB Number
SF-85	Questionnaire for Non-Sensitive Positions	3206-0261
SF-85P	Questionnaire for Public Trust Positions	3206-0191
SF-85PS	Supplemental Questionnaire for Selected Positions	3206-0191
SF-86	Questionnaire for National Security Positions	3206-0005

The forms listed below are attachments that can be uploaded to e-QIP by the applicant/sponsoring agency.

Form Number	Form Name	OMB Number
16A	Specific Release	N/A
SF-171	Application for Federal Employment	3206-0012
OF-306	Declaration for Federal Employment	3296-0182
SF-714	Financial Disclosure Report	3095-0058
OF-612	Optional Application for Federal Employment	3206-0219
ACL	Agency Cover Letter	N/A
ACN	Agency Conducted NAC	N/A
ATA	Agency Attachment	N/A

Form Number	Form Name	OMB Number
ATS	Attachments from Subject	N/A
DHS	Attachment	N/A
FCR	Fair Credit Reporting Disclosure and Authorization	N/A
REL	General Release	N/A
RES	Resume	N/A
CER	Certification Form	N/A
MEL	Medical Release Form	N/A

Section 2. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The e-QIP system collects information directly from the applicant of the investigation. The type of information collected includes: name, address, phone number, aliases used, email, Social Security Number (SSN), Date of Birth (DOB), Place of Birth (POB), citizenship, and personal identifiers. Also collected is detailed information on spouse, cohabitant(s), and immediate family members, such as dates and places of birth and addresses. The system also collects other personal information requested on the forms listed in Section 1.5, such as educational information, financial information, criminal history, and other legal information, medical information, and employment information.

2.2. What are the sources of the information and how is the information collected for the project?

The e-QIP system collects information directly from the applicant either via secure website or via a system-to-system connection with other agencies. In

addition, NBIB and the sponsoring agency personnel can also upload attachments listed in Section 1.5 into the e-QIP website regarding the investigation.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. The e-QIP system does not use information from commercial or publicly available data sources.

2.4. Discuss how accuracy of the data is ensured.

During the collection of the data from the applicant, e-QIP validates that the data provided is appropriately formatted to meet OPM's investigative needs. e-QIP also provides the applicant with formatting instructions and automatic format error messaging to ensure data is entered correctly. Upon completion of the form in e-QIP, applicants certify that their data is complete and accurate, to the best of their knowledge, before releasing the investigation request back to their sponsoring agency.

While sponsoring agencies are primarily responsible for the accuracy of the data, an NBIB document review team validates information received from e-QIP and then a pre-review team validates the information in e-QIP against PIPS for accuracy. This team validates applicant information by comparing basic data, such as name, social security number, and date of birth in the PIPS database.

Once the security questionnaire is completed by the applicant, the sponsoring agency reviews and either accepts or rejects the information provided by the applicant. The information may also be scrutinized by the ISP and returned to e-QIP for correction.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in e-QIP will be inaccurate or incomplete, resulting in an adverse decision for the individual being investigated.

Mitigation: This risk is mitigated by incorporating reviews where NBIB staff validates subject information by comparing basic data, such as name, social security number, and date of birth in the PIPS database. The sponsoring agency has the responsibility to review the information, which has been certified by the subject and submitted to an ISP. If the information is incorrect, or if it includes information not relevant to the investigation, the sponsoring agency returns it to the subject for update/revision. In addition, the e-QIP system further mitigates the risk of misidentification through a requirement that the applicant certify the accuracy of the PII submitted to the e-QIP system.

Section 3. Uses of the Information

3.1. Describe how and why the project uses the information.

e-QIP uses the information collected from the applicant to obtain/verify the necessary information from employers, educational institutions, references, neighbors, associates, police departments, courts, credit bureaus, medical records, probation officials, and prison official to provide a person-centric view of applicants. The information is then used by agency adjudicators to determine if the applicant is suitable or fit for U.S. Government employment; eligible for logical and physical access to federally controlled facilities and information systems; eligible to hold a sensitive positions (including but not limited to eligibility for access to classified information); fit to perform work for or on behalf of the U.S. Government as a contractor employee; qualified for U.S. Government service; qualified to perform contractual services for the U.S. Government; and loyal to the United States.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

No. e-QIP does not use tools, programs, or technology to predict patterns or anomalies.

3.3. Are there other programs/offices with assigned roles and responsibilities within the system?

e-QIP only shares information with U.S. Government agencies, including their contractors, who have a need for the information in the performance of their investigative duties. There are specific agency roles and group roles. Agency roles are focused toward maintaining agency and authorization hierarchy and history, where agency representatives can sponsor individuals to enter data and with authorization can validate past records. Group roles are geared toward validating the information. For example, NBIB FOIA searches the e-QIP system for investigative records to fulfill Privacy Act requests. System Level Roles are Agency User Roles that are granted only to individuals from internal offices such as FOIA, HR, and Security. These System Level Users are not required to have an agency membership in e-QIP in order to access the e-QIP information. The various system level user roles are: e-QIP Agency Support; e-QIP Administrator; e-QIP Access Control; and Freedom of Information Act Administrator..

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk	**Mitigation**

Privacy Risk	**Mitigation**
There is a risk that an authorized person may access the information for an unauthorized purpose and that PII may be accessed or used inappropriately or in a manner not consistent with the original program's purpose or user's specific mission area and authority.	This risk is mitigated by making all users subject to a background check, as well as through annual training. A strongly worded notice is given on a splash screen when users open the application, explaining the expectations, the risks and the consequences. In addition, access controls permit access only to the minimum information that individuals need in the performance of their official duties. PII collected by e-QIP will be used only in accordance with the previously described investigative uses by integrating administrative, technical, and physical security controls that place limitations on the collection of PII and protect PII against unauthorized disclosure, use, modification, or destruction. System users are required to review the Rules of Behavior and complete Annual Security and Privacy Awareness Training. There are also multiple layers of physical and IT cyber protections that are used to safeguard the data. Physical security on the premises ensures that only authorized individuals have access to the building. Layered firewalls and data encryption methods ensure the data can only be accessed by individuals authorized by NBIB Access Control.

Privacy Risk	Mitigation
There is a risk that individuals who do not have a need to know the information in the investigative process will access and use the information for unauthorized purpose.	This risk is mitigated by assigning specific cases and roles to specialized investigators. They can then only see the cases assigned to them, based upon their authorization and privilege. In addition, there are also built in audit logs to monitor disclosures and determine who had access during this time. These logs are checked regularly to ensure that the system is accessed appropriately.

Section 4. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Applicants are provided notice and the ability to consent, in the form of a Privacy Act statement, at the original point of the information collection in e-QIP, and again at the beginning of an in-person interview. They are also told they must provide true, complete, and correct information when completing forms and giving information to investigators and that failure to do so may delay the investigation or the adjudication of the case, and may raise questions concerning eligibility for a security clearance.

Notice is also given in the OPM/CENTRAL 9 SORN and in this PIA.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The standard forms in e-QIP contain Privacy Act Statements, and inform the applicants that providing the information is voluntary, so individuals may decline to provide information or opt out of the project. However, if an individual does not provide each item of requested information, the standard

form will not be submitted and the background investigation cannot be processed.

Applicants do not have the ability, once they have agreed to the background investigation, to consent to some uses of their information and decline to consent to other uses. The exception to this is the SF86 Medical Release authorization, which is valid for 1 year from the date signed but can be revoked at any time by writing to OPM, preventing further collection of medical information covered by that form.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not receive adequate notice concerning how their information is used in e-QIP.

Mitigation: The risk is mitigated by the provision of the Privacy Act Statements on the standard forms listed in Section 1.5 prior to and at the time of information collection, during e-QIP interactions, at the beginning of an in person interview, and other points of collection. While those statements do not explain e-QIP specifically, they do provide information concerning how information will be used. In addition, notification specifically about this system is provided through publication of the OPM/CENTRAL 9 SORN and this PIA.

Section 5. Data Retention by the project

5.1. Explain how long and for what reason the information is retained.

Some records in e-QIP are retained in accordance with the records schedule titled Investigations, which is specific to the Office of Personnel Management (N1–478–08–2, 8 items, 8 temporary items). This schedule addresses retention of records pertaining to OPM NBIB-conducted background investigations, including investigation case files, reports, indexes, adjudications, and appraisals of agency security/suitability investigation programs. In addition, some copies of these records are furnished by NBIB to other agencies, and those records are subject to NARA General Records

Schedule (GRS) 5.6, item 170 and 180 (DAA-GRS-2017-0006-0022), and are required to be destroyed in accordance with NBIB's instructions.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by NBIB staff following the established retention schedule and documented guidance from NARA, which clearly defines retention requirements by record type and agency. All copies of records, both internally and that are sent to other agencies, are maintained only as long as the individual remains of interest to the agency for the purposes defined in the CENTRAL 9 SORN (e.g. suitability, security, credentialing purposes). When the individual is no longer of interest to the agency, NBIB staff are directed to dispose of any/all background investigation records in accordance with its agency-specific NARA regulations, and consistent with documented agreements between the external agencies and NBIB. Each agency is also required by MoUs and ISAs to ensure any retention or re-disclosure of the information does not violate statutory, regulatory, or policy restrictions.

Section 6. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. e-QIP shares information with numerous external agencies that operate as Investigative Service Providers (ISPs) as part of normal operations to conduct background investigations. Government agencies that request ISPs to perform background investigations can also access e-QIP to review the applicant's data before it is provided to any ISP.

Within e-QIP, applicants are allowed to electronically enter, update, and transmit personal investigative data over a secure internet connection to a requesting agency. Then, the requesting agency will review and approve the

investigative data. In addition, the e-QIP system accepts information from external federal agencies via a system-to-system connection.

Appropriate Memorandum of Understanding (MoU) and Interconnection Security Agreement (ISA) document each agency's roles and responsibilities for protecting the data, pursuant with Federal Information Security Management Act (FISMA) 2014 guidelines. The roles and responsibilities associated with access to information are outlined in the MoUs and ISAs.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing described above provides investigatory information for clearance determinations. The determinations include whether an individual is suitable for employment by or on behalf of the Federal government or for military service, or whether an individual is or continues to be eligible for access to national security information. NBIB provides information to its sponsoring agencies to support these determinations. In addition, NBIB provides information to contractors who conduct the background investigations on its behalf. The OPM/CENTRAL 9 SORN contains the following routine uses that permit this sharing and are compatible with the original purpose for the collection:

> (b) To designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government, when such agency, office, or establishment conducts an investigation of the individual for purposes of granting a security clearance, or for the purpose of making a determination of qualifications, suitability, or loyalty to the United States Government, or access to classified information or restricted areas.
>
> (c) To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

(e) To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

(g) To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

6.3. Does the project place limitations on re-dissemination?

Yes. Customer agencies to whom NBIB provides background investigation are limited in their use and re-dissemination of the information, as outlined in MoUs and ISAs. Use and re-dissemination of information by contractors conducting the background investigations for NBIB are limited by the terms of their contracts.

Entities using e-QIP and NBIB systems are also governed by EO 13467, as amended by EO 13764, which allows agencies to release records within the agency and to store subject information for future reference. Each agency is required to ensure any re-disclosure of the information does not violate statutory, regulatory, or policy restrictions. NBIB background investigation records obtained from other agencies may include items that have been disclosed to NBIB with specific re-disclosure limitations. Agencies may coordinate this activity with NBIB's Freedom of Information and Privacy Act office (FOI/PA) Office.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

e-QIP maintains an audit log to track when records are accessed. e-QIP tracks and records access to records following its certification by the applicant or ISP. An Investigative Questionnaire is exported to external agencies during the investigative process. Audit logs track when an applicant starts filling out their standard form. For Agency users, the audit log tracks to whom the form is assigned and each step in the review process.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in e-QIP will be shared with a third party and used or disseminated for a purpose that is not consistent with the purpose for which it was collected.

Mitigation: This risk is mitigated by compliance to the terms documented in MoUs and ISAs, which require the recipients of the information to adhere to all legal and policy requirements related to background investigation information as well as through adherence to the routine uses in the Central 9 SORN and relevant Executive Orders. Note: Specific release forms attached to the standard forms listed in 1.5 permit NBIB to share signed release attachments with third party providers.

Section 7. Redress

7.1. What are the procedures that allow individuals to access their information?

Certain information contained in e-QIP and covered by the OPM/CENTRAL 9 SORN has been exempted from the access and amendment requirements in the Privacy Act. Individuals may request access to any non-exempt information by contacting FOI/PA, Office of Personnel Management, National Background Investigations Bureau, P.O. Box 618, 1137 Branchton Road, Boyers, PA, 16018-0618 or emailing FOIPARequests@nbib.gov. Individuals may submit their request by using Form INV100 Freedom of Information, Privacy Act Record Request Form or by sending the following information: full name, date of birth, place of birth, SSN, mailing address and email address (to receive materials electronically), any available information about the records being requested, a signed and notarized statement or an unsworn statement declaring that the information submitted is true, and copies of two identity documents.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Certain information contained in e-QIP and covered by the OPM/CENTRAL 9 SORN has been exempted from the access and amendment requirements in

the Privacy Act. Individuals may seek to correct non-exempt information by contacting FOI/PA, Office of Personnel Management, National Background Investigations Bureau, P.O. Box 618, 1137 Branchton Road, Boyers, PA, 16018-0618, in writing. Individuals may submit their request by using form INV100 Freedom of Information, Privacy Act Record Request Form or by sending the following information: full name, date of birth, place of birth, SSN, precise identification of the records to be amended, , a statement about and evidence supporting the reasons for the request, including all available information substantiating the request; mailing address and email address to which correspondence should be sent, a signed and notarized statement or an unsworn statement declaring that the information submitted is true, and copies of two identity documents.

7.3. How does the project notify individuals about the

Individuals are notified concerning the procedures for requesting the amendment of records on the NBIB public website, https://nbib.opm.gov/foia-privacy-acts/requesting-an-amending-myrecords/#CopoyofBI, in the published OPM/CENTRAL 9 SORN, and through this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have the opportunity to correct, access, or amend inaccurate information maintained by other agencies and submitted to e-QIP.

Mitigation: This risk is partially mitigated by publishing clear instructions on the NBIB website, in the OPM/Central 9 SORN, and in this PIA to inform individuals about how to access and request amendment to their records. Certain information is exempt from the access and amendment requirements of the Privacy Act; therefore individuals are not able to review or request amendment of that information.

Section 8. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in this PIA?

An individual only has access to e-QIP upon invitation from an authorized agency user and only for a defined period of time. The applicant's access is removed when the time has expired or the applicant has certified and released their data.

The e-QIP system administrators, security administrators, IT specialists, Investigation Service Providers (ISPs), and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based access controls are employed to limit the access of information by users and administrators based on the need to know the information for the performance of their official duties. The e-QIP system enforces separation of duties, preventing unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system.

All customer agencies are bound by MoUs and ISAs that document the appropriate access, use, and dissemination of investigation-related information. In addition, this document and the procedures contained herein are reviewed by the security and privacy offices that allow the agency to make sure information is used in accordance with stated practices.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM/NBIB employees and contractors, having access to the e-QIP system, are required to complete the annual IT Security and Privacy Awareness training.

In addition, e-QIP agency users are not authorized access to the system unless they have completed applicable training required to perform the responsibilities being requested for e-QIP.

First time login instruction, sign-in instruction and a guide for the Standard Form 86 are also provided on the NBIB and e-QIP web pages that can be found at https://nbib.opm.gov/e-qip-background-investigations. There are also frequently asked questions (FAQs) for the users, regarding the use of e-QIP, NBIB and the information needed on the standard forms.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to any part of the system is approved specifically for, and limited to, users who have an official need to know the information for the performance of their investigative duties. NBIB access control officials determine who needs access to the system and the NBIB Access Control grants access based on need to know and business role. In order to receive access, individuals must be U.S. citizens and undergo an appropriate background investigation.

All ISP access requests are submitted in writing to the NBIB Access Control Team, who validates and grants access and designates a system administrator to provide access to approved ISPs. Various roles within the system require different levels of background investigation as defined by NBIB Policy Team. Each role has a minimum background investigation level and is enforced by the restrictions included in the MoU and ISA.

An individual only has access to the e-QIP application upon invitation from an authorized agency user and only for a defined period of time. The applicant’s access is removed when the time has expired or the applicant has certified and released their data.

Numerous other security measures have been built into e-QIP to prevent unauthorized access to information, including two-factor authentication e-QIP also uses layered security and common cryptographic protocols to ensure secure end-to-end transit at the transport layer. All internet-based data transmissions are encrypted using encryption provided through common browser SSL technology.

The system requires certain secure measures are enabled in the user's browser. Without this setting users receive a "Page Cannot be Displayed" error message. During the initial log in to e-QIP, each user must first answer a series of unique questions about basic demographic information they provided to the sponsoring agency, along with a Registration Code. After successfully answering these questions, users must create a unique username and password. Finally, they must create a set of three challenge questions that they will need to respond to in the event they need to reset their password. If users have issues with logging in, they must contact their sponsoring agency for assistance and not call NBIB directly.

Only persons with active investigation requests can log in to e-QIP. e-QIP has been tested through the National Institute of Standards and Technology (NIST) Certification and Accreditation process and is compliant with all requirements. It is NBIB policy to ensure that all IT systems that collect, maintain, or disseminate information in an identifiable form have Federally mandated controls in place to protect and prevent the breach of PII.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The NBIB staff reviews the MoUs and ISAs every three years for renewal and makes any necessary adjustments. Any new access to e-QIP will be evaluated by the appropriate NBIB personnel and documented in a MoU or ISA, which is approved by the OPM Chief Information Security Officer (CISO). New uses of the information are business decisions determined by the NBIB Information Technology Management Office, in coordination with relevant stakeholders.

Responsible Officials

Charles S. Phalen, Director
National Background Investigation Bureau

Approval Signature

_____

Kellie Cosgrove Riley
Chief Privacy Officer