Privacy Impact Assessment for the

Personnel Investigations Processing System (PIPS)

October 4, 2017

Contact Points

Eric J. Riutort
System Owner
Office of Personnel Management
OCIO/NBIB ITPMO

Roy Parkinson
Product Owner
NBIB/ITMO/PO

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer
Office of Personnel Management

Abstract

The United States Office of Personnel Management National Background Investigations Bureau conducts background investigations, reinvestigations, and continuous evaluations of individuals under consideration for, or retention of, Government employment. The purpose of Personnel Investigations Processing System (PIPS) is to allow for an automated entry, scheduling, case control, and closings of background investigations and to store the important information to be used in security and suitability programs and decisions. This PIA is being conducted because PIPS contains personally identifiable information about individuals who are undergoing a background investigation and about others whose information may be included in background investigation files.

Overview

The United States (U.S.) 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 over 2 million 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 OPM and to external agencies. The PIPS system is a central information portfolio that supports the implementation of the investigations and assists in report generation.

The NBIB Background Investigation mission consists of the following major general processes which involves many systems. The process begins when a candidate is identified for investigation. At this time, the investigation is initiated and an application is completed and submitted by the candidate, then the application is reviewed and screened. From this point, an investigation is scheduled, assigned, and then conducted, resulting in various Reports of Investigation (ROI). The OPM Staff conducts the examination of the ROI and a general case review. Once evaluated, the case is closed and the Distributed Investigative File (DIF) is produced and sent to the agency sponsoring the investigation for its decision. Ultimately, the investigation data is maintained, retained, or purged (as appropriate) from the various systems that are required for the investigative process.

For PIPS, its involvement starts when the external agency user validates the need for the investigation and initiates a request in the e-QIP system, or collects biometric information from the subject and transmits to the Fingerprint Transaction System (FTS). e-QIP is a secure OPM-based website designed to automate the common background investigation questionnaires (national security, public trust, and non-sensitive questionnaires or security and suitability) used to process Federal background investigations. FTS handles fingerprint checks by providing a

secure means for approved agencies to submit electronic or hard cards fingerprint images for the Federal background investigations. That information is then transmitted to PIPS and a case is created. It is then screened for completeness and a background investigation is scheduled. Automated scheduling scopes the case and identifies the items required that, once collected, is compiled into ROIs and sent to adjudicative agencies as a DIF package.

PIPS is an automated system that houses the Security/Suitability Investigations Index (SII) and is used for the automated entry, scheduling, case control and closing of background investigations. SII is the repository of personnel investigations conducted by OPM and other authorized agencies. PIPS uses information from the SII to support the process of conducting investigations and to facilitate reciprocity. The need for reciprocity and processing includes: data-entry of security questionnaire information on individuals who are being investigated; automated scheduling of National Agency Checks (NACs) at the Federal Bureau of Investigation (FBI), Department of Defense Central Index of Investigations (DCII), national credit bureaus, and various other sources necessary for a complete investigation. PIPS facilitates scheduling and transmitting investigation requests to investigators, receiving reports of investigation from investigators, closing investigations, and transmitting results electronically to customer agencies.

Through automated linkages, such as the Central Verification System (CVS), PIPS provides an agency's security office with direct access to the investigation information relevant to their agency. CVS is used to hold civilian clearance, polygraph and Homeland Security Presidential Direction 12 (HSPD-12) information for the applicable agencies. This direct linkage reduces an agency's processing time by replacing mailed forms and eliminating the need to make telephone inquiries. Security offices can conduct online SII searches, request files, transmit messages, record notifications, enter Special Agreement Checks, and monitor the progress of cases. PIPS also enables the tracking of all stages and pieces of every investigation initiated by NBIB. From the data in PIPS, NBIB produces various reports used by both NBIB and its customer agencies to track investigations.

Also, in order to ensure investigative data is maintained and purged properly, the Retention of Investigative Data (ROID) is incorporated into PIPS as a backend application. The ROID application consists of scheduled batch jobs that purge and archive investigation data in accordance with National Archives and Records Administration (NARA)-approved retention schedules. ROID addresses investigative data for applicant and investigation, ROI, Case Data, Credit Reports, Federal Bureau of Investigation (FBI) Fingerprint Results, PIPS Billing History Files, and associated reports/messages.

Section 1.0 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, OPM 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)) applies to the information?

The SORN that applies is OPM/Central 9 Personnel Investigations Records which can be located at: https://www.gpo.gov/fdsys/pkg/FR-2016-10-11/html/2016-24507.htm.

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

Yes, the PIPS System Security Plan (SSP) was completed as part of the system's Authority to Operate on January 20, 2017.

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

Yes, the records in PIPS are covered by the records schedule titled Office of Personnel Management, Federal Investigative Services Division (N1–478–08–2, 8 items, 8 temporary items), which addresses retention of records pertaining to the government-wide security background investigation program, including investigation case files, reports, indexes, adjudications, and appraisals of agency security/suitability investigation programs.

In addition, the copies of these records that NBIB furnishes to another agency are subject to NARA General Records Schedule (GRS) 5.6, item 170 (DAA-GRS-2017-0006-0022), and should be destroyed in accordance with NBIB's instructions.

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.

PIPS incorporates information that individuals record on the forms listed below, such as the questionnaire for non-sensitive positions, national security positions, and fingerprint chart respectively. The Office of Management and Budget (OMB) control numbers for the initial collections are:

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
SF-86A	Questionnaire for National Security Positions	3206-0007
SF-86C	Standard Form 86 Certification	3206-0005
SF-87	Fingerprint Chart	3206-0150

Section 2.0 Characterization of the Information

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

PIPS maintains information pertaining to the individuals who are the subject of an investigation, including: first name, last name, address, phone number, aliases used, Social Security Number (SSN), Date of Birth (DOB), Place of Birth (POB), educational information, financial information, personal conduct, legal information, medical information, employment information, and other information requested on the forms listed in Section 1.5. In addition, in certain circumstances, name, address, phone number, SSN, DOB, and POB for the individual's immediate family members, former spouses, and cohabitants is also maintained, as well as information about others whom the individual identifies or who are identified by the investigator during the course of the investigation. Also, it contains other data that is collected or developed in the course of investigation, which is information that is part of the subject's personal history.

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

The information in PIPS is obtained from a variety of sources. Individuals enter information on required security questionnaires through e-QIP, which is then automatically ingested into PIPS. They also provide information to Federal and contractor investigators during personal interviews. The investigators submit that information through PIPS in the form of a ROI.

Other information in PIPS is obtained from conducting electronic records searches, mailing verification requests or inquiries to relevant entities or individuals, reviewing records at repositories, and interviews. Specific sources of information include employers, educational institutions, references, neighbors, associates, police departments, courts, Consumer Reporting Agencies, medical records, probation officials, prison officials, and newspapers, magazines, and other publications, and license information from licensing bureaus.

Consistent with Federal investigation standards, some of the information contained in PIPS comes from other agencies and commercial entities via automated National Agency Checks (NAC), including but not limited to: the Federal Bureau of Investigation (FBI) Fingerprint-based Criminal History Check, FBI Name Check (Background Investigations), Defense Central Investigative Index, Selective Service System, U.S. Citizenship and Immigration Services, Financial Crimes Enforcement Network (FINCEN), Consumer Reporting Agencies, and the National Crime Information Center (NCIC). Some of the data flows to PIPS through other NBIB systems, such as Non-Field Work (NFW), which is a system that connects to outside entities.

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

Yes. PIPS has electronic connections with various commercial and publicly available NAC repositories, including the national consumer reporting agencies, to request information about individuals. The use of commercial sources serves as relevant data points, which can vary depending on the nature of the position an individual is seeking, to obtain a comprehensive picture of the individual during the investigative process. Commercial sources are utilized consistent with the Federal investigative standards and in accordance with applicable law, such as the notice requirements of the Fair Credit Reporting Act.

2.4 Discuss how accuracy of the data is ensured.

Information collected in the course of the background investigation is verified through review of corroborating records. The information may be checked by a group of reviewers who validate that the information is about the individual being investigated and is pertinent to the investigations process. The information may also be further scrutinized by a team of investigation case analysts who review the cases, validate, and verify responses from individuals. This team looks for anomalies or errors by reviewing the information obtained from third party sources and comparing it against information provided by the individual.

In addition, the ROID application is used to maintain and purge investigative data in accordance with OPM and other Federal policies, contributing the timeliness, relevance, and accuracy of information in PIPS.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information obtained in the course of the investigation will be inaccurate, resulting in an adverse decision for the individual being investigated.

Mitigation: This risk is mitigated by incorporating reviews by a team of case analysts who confirm that the information pertains to the individual being investigated and corroborate the information using various sources.

Privacy Risk: There is a risk that information obtained from commercial sources and electronic records searches will be misinterpreted or that relevant information may be overlooked, resulting in an adverse decision for the individual being investigated.

Mitigation: This risk is mitigated by training investigators regarding how to interpret the information they obtain in the course of the investigation and by having processes in place to validate the information. The risk is also lessened by using the ROID application, a backend application consisting of scheduled batch jobs that purge and minimize investigation data in accordance with NARA-approved retention schedules. The system runs on an automatic schedule daily, weekly, or monthly, with two additional on-demand jobs that purge an individual's data when it is no longer timely.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Information collected and processed in PIPS is used by agency adjudicators to determine an individual's suitability/fitness for Federal employment and/or a position of trust with the Federal government, and/or for eligibility and access determinations. The information collected about the individual in the course of the investigation is used to ensure that any person employed by the Federal government is reliable, trustworthy, of good conduct and character, and loyal to the United States.

3.2 Does the project use tools, programs, or other 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.

PIPS is programmed to schedule required searches, interviews, and personnel coverage based on the type of investigation requested and the type of information needed (e.g., residence, employment, education). There are no tools, programs or other technologies used to conduct electronic searches, queries or analyses.

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

Within OPM, only personnel and contractors in NBIB who have a need for the information in the performance of their job duties have access to PIPS. NBIB personnel and contractors are responsible for processing background investigations from the time the request to do the investigation is obtained from the customer agency, closing out the investigation, overseeing the background investigations processes, and releasing the investigations, as appropriate, pursuant to the Privacy Act and the Freedom of Information Act.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that individuals who do not have a need to know the information in PIPS will access and use the information for unauthorized purpose.

Mitigation: This risk is minimized through the use of access controls that permit access only to the minimum information that individuals need in the performance of their official duties.

Privacy Risk: There is a risk that authorized users may inappropriately access and disclose the information in PIPS for an unauthorized purpose.

Mitigation: This risk is mitigated by assigning specific cases and roles. 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 was is accessed appropriately.

Privacy Risk: There is a risk of loss or compromise of sensitive information collected through the background investigation process.

Mitigation: This risk is mitigated through the use of multiple layers of physical and IT protection used to safeguard the data. In addition, physical security on the premises ensures that only authorized individuals have access to the building and layered firewalls and data encryption methods ensure it can only be access by authorized individuals on the network.

Section 4.0 Notice

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

PIPS is not accessible by individual members of the public and, therefore, does not provide direct notice of its collection of information to individuals. However, subjects of investigation are provided notice, in the form of a Privacy Act statement, at the original point of the information collection in the e-QIP system, 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. Individuals are also informed that they may also be denied employment, fired from the job, or debarred from Federal employment for making false statements. Sources (not subjects of investigation) are also provided a Privacy Act advisement when interviewed in-person and when asked to complete an investigative inquiry. Both subjects of investigation and sources are informed concerning why the information is being collected and how it will be used.

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 all uses, decline to provide information, consent to particular uses of the information, or opt out of the project?

Individuals are notified at the point of collection via the e-QIP system, at the beginning of an in person interview, and on various consent forms that providing information is voluntary but that if they do not consent to the collection of the required information, it may affect the completion of their background investigation. They 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 the U.S. 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 will not receive adequate notice concerning how their information is being used in PIPS.

Mitigation: This risk is mitigated through the notice that individuals receive at the point of collection via the e-QIP system, and again at the beginning of an in person interview. While that notice does not explain PIPS, it does provide information concerning how their information will be used. In addition, notification specifically about PIPS is provided through publication of the OPM/Central 9 SORN and this PIA.

Section 5.0 Data Retention by the project

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

PIPS follow the retention schedule referenced in Section 1.4. Depending on the type of information and the action taken on that information, various retention periods apply. Standard investigations with no issues are retained for 16 years from the closing of the investigation; those with issues are retained for 25 years from the closing of the investigation. Files obtained from other agencies in the course of an investigation are retained consistent with the agreement between the agency and OPM.

Copies of records the NBIB provides to another agency may be 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). Upon separation or when the individual is no longer of interest to the agency, the agency must dispose of any/all background investigation records.

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.

Section 6.0 Information Sharing

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

Yes. NBIB conducts background investigations for its customer agencies, including the Department of Defense and civilian agencies, and provides copies to designated agency officials for use in making determinations concerning whether an individual is suitable or fit for Federal government employment; eligible for logical and physical access to federally controlled facilities and information systems; eligible to hold a sensitive position (including but not limited to eligibility for access to classified information); fit to perform work for or on behalf of the government as a contractor employee; qualified for government service; qualified to perform contractual services for the government; and loyal to the United States. For example, NBIB uses PIPS to facilitate the exchange of security clearance and background investigation information with the Defense Security Service (DSS) Joint Personnel Adjudication System (JPAS). In addition, reports of background investigation information are provided electronically, using PIPS, to customer agencies who register to receive the results of the background investigations relevant to their agencies.

In order to gather and maintain the relevant information required to conduct a background investigation, PIPS interfaces with and incorporates other systems and provides information about the individual subject in order to obtain, for example, information from consumer reporting agencies, other federal agencies, employers, and friends and family. Another interface is the on-line CVS. It is used to hold civilian clearance, polygraph and HSPD-12 (PIV Card) information for the applicable agencies. External agencies use a specialized web portal to add and/or modify the CVS data in PIPS. These are secured, batch upload processes checking the availability of agency files and performing validation and upload processes.

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 is compatible with the purpose for which the information was collected, which is, in part, to provide investigatory information for determinations concerning whether an individual is or continues to be suitable or fit 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 customer agencies so that they may make such determinations and provides information to others in order to collect all the information necessary to make those determinations. In addition, NBIB provides information to contractors who conduct the background investigations on its behalf. The OPM/Central 9 SORN contains routine uses that permit this sharing and are compatible with the original purpose for the collection. These include, in particular, routine uses a, c, e, and g:

- (a) To designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government or the Government of the District of Columbia having a need to investigate, evaluate, or make a determination regarding loyalty to the United States; qualifications, suitability, or fitness for Government employment or military service; eligibility for logical or physical access to federally-controlled facilities or information systems; eligibility for access to classified information or to hold a sensitive position; qualifications or fitness to perform work for or on behalf of the Government under contract, grant, or other agreement; or access to 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 an agency, office, or other establishment in the executive, legislative, or judicial branches of the Federal Government in response to its request, in connection with its current employee's, contractor employee's, or military member's retention; loyalty; qualifications, suitability, or fitness for employment; eligibility for logical or physical access to federally-controlled facilities or information systems; eligibility for access to classified information or to hold a sensitive position; qualifications or fitness to perform work for or on behalf of the Government under contract, grant, or other agreement; or access to restricted areas.
- (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 memoranda of understanding and information sharing agreements. Use and re-dissemination of information by contractors conducting the background investigations for OPM NBIB are limited by the terms of their contracts.

Customer agencies are also governed by EO 13467, as amended by EO 13764, which allows the agencies to release records in coordination with the NBIB Freedom of Information and Privacy Act office (FOI/PA). This coordination is required to ensure any re-disclosure of the information does not violate any statutory or other restrictions, as certain NBIB background investigation records obtained from other agencies do include items that have been disclosed to NBIB with re-disclosure limitations.

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

PIPS tracks disclosures by keeping a log of the activity within the system. These logs are reviewed regularly and can be accessed as needed to account for the disclosure of an individual's information.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in PIPS 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 entering into MoUs and ISAs that require the recipients of the information to adhere to all legal and policy requirements related to background investigation information.

Section 7.0 Redress

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

Certain information contained in PIPS 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 individual to correct inaccurate or erroneous information?

Certain information contained in PIPS 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 procedures for correcting their information?

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-and-amending-my-records/#CopyofBI, in the published OPM/Central 9 SORN, and through this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Because PIPS is not a public system and individuals do not have direct access to their information in PIPS, there is a risk that individuals will not understand how to request access to and amendment of their records.

Mitigation: This risk is 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. However, certain information is exempt from the access and amendment requirements of the Privacy Act and individuals will not be able to review or request amendment of that information.

Section 8.0 Auditing and Accountability

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

Role-based access controls are employed to limit access to the information in PIPS to system users and administrators based on the need to know the information for the performance of their official duties. PIPS also employs processes to enforce separation of duties, to prevent unauthorized disclosure, and to prevent modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system.

In addition, all customer agencies are bound by MoUs and ISAs that document the appropriate access, use, and dissemination of the information in PIPS

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

All OPM/NBIB employees and contractors who have access to PIPS are required to complete the annual IT Security and Privacy Awareness training. PIPS users are not authorized access to the system unless they have completed applicable training required to perform the responsibilities being requested for PIPS.

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

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

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?

NBIB staff review the MoUs and ISAs every three years to renew and make any necessary adjustments. Any new access to PIPS will be evaluated by appropriate NBIB personnel and documented in a MoU or ISA approved by NBIB leadership. New uses of the information are business decisions determined by NBIB leadership in coordination with relevant stakeholders.

Responsible Officials

Charles S. Phalen, Director
National Background Investigations Bureau

Approval Signature

Signed copy on file with the OPM Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer
Office of Personnel Management