Privacy Impact Assessment
for the

OPM PIPS Imaging System (OPIS)

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 OPM Personnel Investigations Processing System Imaging System (OPIS) is to provide NBIB with specialized secure document control and information management services that directly support the operation of NBIB. This Privacy Impact Assessment (PIA) is being conducted because OPIS contains 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

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 the 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 Questionnaire for Investigations Processing (e-QIP), a system that provides a means to facilitate the processing of standard investigative forms.

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). 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

The purpose OPIS, the subject of this PIA, is to provide NBIB users with the ability to create, process, and produce standardized individual security investigation and background check products in a near-paperless work environment. The OPIS system allows NBIB personnel to electronically retrieve, modify, and store case documents that were previously only available on paper. The primary focus of OPIS is to provide imaging services in the form of paper to electronic document conversion, quality assurance, image storage and retrieval, and image release components.

There are multiple ways OPIS receives paper and electronic documents. The paper documents are received through the mail room and placed in lockboxes. The lockboxes are carried over to an imaging room for electronic scanning into OPIS. Electronic files are received from e-QIP, consumer reporting agencies, educational institutions, law enforcement agencies, and others and then ingested into OPIS.

Once a case is closed, OPIS packages the appropriate documents for electronic delivery (eDelivery) to the sponsoring agency.

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, the 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 records contained in OPIS is OPM/CENTRAL 9 Personnel Investigations Records which can be found at www.opm.gov/privacy.

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

Yes. The OPIS System Security Plan (SSP), Version 1.2, November 25, 2016, was completed as part of the system's Authority to Operate (ATO) on January 20, 2017. It was last updated to Version 3.0 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, items 170.

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.

OPIS contains images of the following standard forms and related supplemental request forms within the standard forms, which it obtains via e-QIP.

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	Continuation Sheet for Questionnaires	3206-0007
SF-86C	Standard Form 86 Certification	3206-0005
SF-714	Financial Disclosure Report	3095-0058
OF-306	Declaration for Federal Employment	3296-0182

In addition, the forms listed below are also artifacts that OPIS contains, obtained from various sources, some of which are covered by the PRA as indicated.

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

Form Number	Form Name	OMB Number
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
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
A03360	Case Activity Memorandum	N/A
A04	Security Suitability Investigation Index	N/A
N/A	Various of Release forms	N/A
FD-258	Fingerprint Card (Unclassifiable Only)	N/A
821	IRS Tax Release	N/A
397	Education Verification Notice	N/A
254	Credit Notice	N/A
70B	Investigative Record Amend	N/A

Form Number	Form Name	OMB Number
313	Protected Source Identification Sheet	N/A

Section 2. Characterization of the Information

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

OPIS collects, uses, disseminates, and maintains images of the forms listed in Section 1.5 as well as other artifacts obtained from e-QIP, the requesting agency, NBIB Investigator or external sources in the background investigation process. These images contain PII about the subject of the investigation, including 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 applicable forms and during the investigative process. In addition, in certain circumstances, the forms imaged contain the name, address, phone number, SSN, DOB, and POB for the individual's immediate family members, former spouses, and cohabitants, as well as information about others whom the individual identifies or who are identified by the investigator during the course of the investigation. OPIS also compiles and maintains a Distributed Investigative File (DIF), which is a compilation of releasable documents that are electronically transmitted to the customer agency.

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

There are multiple ways OPIS receives paper and electronic documents. Paper documents are received from a variety of sources, including the subject of the investigation, handwritten Investigator notes, documents Investigators obtain during investigation and external sources that are received in the mail room and placed in lockboxes. The lockboxes are carried over to imaging room for electronic scanning into OPIS. Electronic

files are received from e-QIP, consumer reporting agencies, educational institutions, law enforcement agencies, and others and then ingested into OPIS.

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. OPIS manages and stores images from various commercial and publicly available NAC repositories, including the national consumer reporting agencies. 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.

OPIS performs image quality checks during the scanning process to ensure that the images are clear, and NBIB personnel do verify that subject identifiers (such as name, SSN, and DOB) for case documents stored in OPIS match with information in PIPS, but OPIS does not check the information for accuracy.

Outside of OPIS the following takes place, 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. OPIS assumes that the information contained in the documents stored has been properly vetted by the responsible parties submitting previously mentioned documents.

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 or incomplete and result in an adverse or incorrect decision regarding the individual being investigated.

Mitigation: This risk is partially mitigated in OPIS by incorporating reviews during which OPIS validates subject information by comparing basic data, such as first name, last name, SSN, DOB, and POB in the PIPS database. In addition, the risk of inaccuracy and incompleteness is mitigated throughout the investigative process as described in Section 2.4. During the collection of the data from e-QIP, there are steps taken to validate that the data provided is appropriately formatted to meet NBIB's investigative needs. NBIB's e-QIP system provides all applicants with formatting instructions and automatic format error messaging to ensure data is entered correctly. Upon completion of the form in e-QIP, the applicant certifies that their data is complete and accurate, to the best of their knowledge, before releasing the investigation request back to their sponsoring agency. The sponsoring agency is then responsible to check the accuracy of the data.

Section 3. Uses of the Information

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

Authorized NBIB employees and contractors review the documents in OPIS as part of their investigative responsibilities. These include quality and subject validation or checks. During the course of the investigation, authorized users can make appropriate updates to the imaged documents. Once an investigation is closed, OPIS returns a specified set of images back to the requesting agency either in hard copy or through eDelivery. Information collected and processed in this system 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 of America.

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. OPIS does not use tools, programs, or technology to predict any patterns or anomalies.

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 OPIS and the information contained therein. This includes authorized investigative contractors, who have a need for the information in the performance of their investigative duties.

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

Privacy Risk: There is a risk that PII maybe be accessed or used inappropriately or in a manner not consistent with the original purpose for which it was collected or with the user's specific mission area and authority.

Mitigation: This risk is mitigated by creating dedicated user roles established by NBIB investigations policy. Access controls permit access only to the minimum information that individuals need in the performance of their official duties. PII stored or transferred must only be used in accordance with the investigative process. Measures that integrate administrative, technical, and physical security controls 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.

Privacy Risk: 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.

Mitigation: 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 was 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.

OPIS is a NBIB internal system not accessible by the public and/or individuals, therefore, notice is not given by the system itself. However, subjects of investigations are provided notice via Privacy Act statements at the original point of the information collection, 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 when providing information to investigators; and that failure to do so may delay the investigation or the adjudication of their 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?

Individuals are notified at the point of collection, at the beginning of an in person interview, and on various consent forms. They are informed 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 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 OPIS.

Mitigation: This risk is mitigated by the provision of the Privacy Act Statement when information is collected from the individuals. While that statement does not explain OPIS specifically, it does provide information concerning how their information will be used. In addition, notification 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.

The records in OPIS are subject to 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 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). This is consistent with GRS 5.6 170 (Disposition Authority - DAA-GRS2017-00060022). 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. 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 the 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. Once an investigation is closed, OPIS returns a specified set of images for eDelivery back to the sponsoring agency via secured connection. Appropriate MoUs and ISAs document each agency's responsibilities to protect the data in compliance with Federal Information Security Management Act (FISMA) 2014 guidelines. Roles and responsibilities regarding 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 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. 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:

(a) To designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government, having a need to evaluate qualifications, suitability, and loyalty to the United States Government and/or a security clearance or access determination.

(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 designated officers and employees of agencies, offices, and other establishments in the executive, judicial, or legislative branches of the Federal Government, having the responsibility to grant clearances to make a determination regarding access to classified information or restricted areas, or to evaluate qualifications, suitability, or loyalty to the United States Government, in connection with performance of a service to the Federal Government under a contract or other agreement.

(k) For agencies that use adjudicative support services of another agency, at the request of the original agency, the results will be furnished to the agency providing the adjudicative support.

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 OPIS 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 the Bureau'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.

OPIS tracks disclosures by keeping a log of the data change activity specific to a case (i.e., data additions, deletions, and revisions) as well as of the dissemination of the documents released to the sponsoring agency.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in OPIS 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 by adherence to the OPM/CENTRAL 9 SORN. Note: Specific release forms attached to the standard forms listed in Section 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?

Individuals from the public have no direct access to the information in the OPIS and certain information contained in OPIS and covered by the OPM/CENTRAL 9 SORN has been exempted from the access and amendment requirements in the Privacy Act. However, 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?

Individuals from the public have no direct access to the information in OPIS and certain information contained in OPIS and covered by the OPM/CENTRAL 9 SORN has been exempted from the access and amendment requirements in the Privacy Act. However, 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 shared to OPIS.

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 access 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?

The OPIS 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. OPIS 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 in coordination with the OPM Security and Privacy Policies Handbook Version 3, March 31, 2011 and the updated addendum policies.

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 regularly 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 with access to OPIS are required to complete the annual IT Security and Privacy Awareness training. The OPIS system users are not authorized access to the system unless they have completed applicable training required to perform the responsibilities being requested for the OPIS system. In addition, training guides specific to OPIS are accessible to authorized users from the OPIS home page and Field Document Repository (FDR) training is also provided by NBIB as part of the investigator training course.

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 OPIS is approved specifically for, and limited to, users who have an official need to know the information for the performance of their investigative duties. The NBIB access control officials determine access to the system, and 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.

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 or necessary adjustments. Any new access to the OPIS 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 (ITMO), in coordination with relevant stakeholders.

Responsible Official

Charles S. Phalen, Director
National Background Investigation Bureau

Approval Signature

Signed Copy on File with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer