Privacy Impact Assessment
for the

NBIB Public Portal
(NP2)

April 18, 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 NBIB Public Portal (NP2) is to provide internal/external agency customers/partners with a secure, multi-factor authenticated means of communication with NBIB systems based on roles and responsibilities. This Privacy Impact Assessment (PIA) is being conducted because the NP2 system 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

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 NBIB Public Portal (NP2) provides authorized users with a closed, secure communication system that requires Personal Identity Verification (PIV)/multi-factor authentication for access. NP2 enables authorized users to access the following: the NP2 Document Repository, e-QIP, the CVS Batch File Submission Tool, PIPS/CVS, the NBIB Invoice tool, and NP2's Messaging function.

The NP2 Document Repository contains both public and private libraries. Documents in the public library can be accessed by all authorized NP2 users and consist of common NBIB business information. Public library documents include Federal Investigative Notices, which provide policy and guidance regarding the investigative process, and Job Aids, which provide NBIB customers specific instructions regarding various NBIB system functions. For example, Job Aids have been created to instruct agency users on how to initiate investigative requests in e-QIP or how to post adjudicative information in the Central Verification System (CVS), a component of PIPS. The OPM form 70b, used to request access to CVS, is also available in the public library as are hard copy versions of the SF86 and SF85 forms.

Within the Document Repository, private libraries are used to share more sensitive information, such as sensitive PII and case-specific information, which may include credit information, criminal history information, military records, and other information that is part of the Background Investigation. An individual who needs to collaborate with other users regarding such

sensitive documents has the ability to create a private library and grant access to other authorized users. The use of NP2 to share and discuss documents in a closed and secure environment eliminates the need to email documents or share hard copies in a less secure environment. Private libraries that contain sensitive PII are tagged when created and the information is automatically deleted at regular intervals once the need for collaboration has ended.

NP2 also enable agency administrators to access e-QIP in order to review its applicants' data and manage access for its users. This agency access through NP2 is different than the interface an individual applicant has to e-QIP and is used by agency users to initiate, review, approve and then release to NBIB requests for investigation in e-QIP.

The CVS Batch File Submission tool in NP2 allows users to submit text files to add or update a large number of records in the CVS at one time. Authorized users from NBIB customer agencies use this tool to report or update clearance information in CVS or to request information about cleared individuals. The tool includes both the ability to upload batch files and the ability to receive and download the results of any requests related to the upload. In addition to the ability to submit batch files to CVS, NP2 also provides a secure connection for NBIB customers to directly access PIPS/CVS.

The NP2 Invoice tool is designed to allow self-service access of NBIB customer to their invoice files. Invoices are pushed to NP2 from PIPS via the Consolidated Business Information System (CBIS) on a monthly bases. Authorized users from the agencies access their invoices in NP2. NP2 users may access only the current and previous fiscal year's invoices, thought he invoices are retained in the system for a period of five years. The invoice files contain the receipt of work completed by NBIB for the respective customer agencies.

The Messaging function in NP2 is a communication tool that is used for composing, sending and receiving email between NP2 users in a closed and secure environment. Messaging is unable to send email outside of the NP2 environment and authorized users are only able to send messages to other authorized users of NP2. Common uses of Messaging are the delivery of sensitive reports, metrics, credit reports, and access requests, the

submission of access requests as attachments, and support of users of NBIB systems.

The request for NP2 System access is initiated through designated supervisory channels of the potential user based upon their business responsibilities. NBIB access control officials evaluate and determine access to the system and the NBIB security office grants access based on need to know and business role. When an NP2 user accesses the system, they can only see those aspects of the system that they have a need-to-know. For example, if a user only has a business need to conduct administrative activities in e-QIP, that user will not see or have access to PIPS/CVS through NP2. In addition, access through NP2 is dependent upon system-level access. As a result, no authorized NP2 user can access e-QIP or PIPS/CVS, for example, through NP2 unless NBIB access control officials have separately granted access to e-QIP or PIPS/CVS.

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 NP2 is OPM/CENTRAL 9 Personnel Investigations Records.

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

Yes. The NP2 System Security Plan (SSP), Version 1.0, December 2017, was completed as part of the system's Authorization to Operate (ATO) on January 20, 2017. It was last updated to Version 3.5 on December 2017 as part of the upcoming system re-authorization.

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

Yes. The records schedule for investigative records is N1-478-08-002.

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.

The NP2 system does not collect information directly from individuals; however, some of the information that NP2 permits users to access in other systems, such as PIPS and e-QIP, is covered by the PRA. For example, e-QIP collects information via the forms listed below:

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

Section 2. Characterization of the Information

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

The NP2 system enables users to access e-QIP and PIPS/CVS as well as to create private libraries and communicate with other NP2 users concerning background investigations. The information in the private libraries and messages will vary but may include information about the subject of a background 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.

The NP2 system also stores invoice information, which contains general information about the background investigation and the agency requesting the investigation, as well as certain information about the subject of the investigation, including name and SSN.

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

The information in the NP2 system is obtained from other NBIB and OPM systems, such as e-QIP, PIPS/CVS, and CBIS. Those systems obtain the information from a variety of sources, including the individual subject of a background investigation, electronic records searches, interviews, and National Agency Checks (NACs).

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

The NP2 System does not retrieve information from commercial or publicly available data, but the information it obtains from other systems may include commercial or publicly available information.

2.4. Discuss how accuracy of the data is ensured.

The NP2 system does not independently ensure the accuracy of the information it contains and the relevance and accuracy of the documents shared between one or more users within the public and privacy libraries is the responsibility of the users.. However, 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.

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

Privacy Risk: There is a risk that the information in the system may not be accurate, resulting in an adverse decision or unnecessary additional vetting for the subject of the background investigation.

Mitigation: This risk is partially mitigated by the validation and accuracy checks that occur in the systems from which NP2 obtains information. It is also partially mitigated by training system users to understand the relevance of the information they access in NP2 and that they place in private libraries and communicate in the messaging functionality.

Section 3. Uses of the Information

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

NP2 provides authorized users with a closed, secure communication system and secure access to e-QIP and PIPS/CVS. The system was created to replace legacy communications with automated connections with more modern, flexible, customizable, and robust technology.

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. The NP2 system does not use technology to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or anomaly.

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 NP2 and the information contained therein. Externally, 300 plus agencies have access to the NP2 system, based on their respective need-to-know. Requests to create a user account for NP2 pass through supervisory channels to the NBIB Access Control Branch for approval and creation. Every user is granted, as a minimum, the General User role, which allows access to the NP2 portal, the internal NP2 messaging function between users, access to public folders, and creation and sharing of private folders for collaboration in the investigation process. Additional roles created under the NP2 System are: System Administrator to perform maintenance of the system, Portal Administrator and Content Manager to conduct administrative functions within the portal, Invoice User and Invoice Administration User which permit access to NBIB's invoicing system, CVS Batch File User and CVS Batch File Administrator which permit access to the PIS/CVS, and finally e-QIP User which allows access to the e-QIP system.

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 program's purpose or 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. System users are required to review the Rules of Behavior.

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

Mitigation: This risk is mitigated by assigning specific roles to business users. They can only access those functions to which they are granted entitlement by their role. The approval for this access goes through a multi-tiered process starting with their authorized supervisor who is responsible for establishing their access and need-to-know and then proceeding to the NBIB Access Control Branch for final disposition. In addition, audit logs are maintained that track all aspects of user creation, privilege changes, and user interaction with the system. This logging records who accessed the system, the time and duration of the access, and what was accessed by the user.

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.

NP2 is not accessible by individuals who are subjects of a background investigations 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 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. Accordingly, they cannot decline to provide consent for the inclusion of their information in NP2.

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.

Mitigation: This risk is partially mitigated by the provision of the Privacy Act Statement when information is collected from the individuals. While that statement does not explain NP2 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 the system are retained in accordance with the NARA records schedule identified in Section 1.4.

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 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.

Over 300 external agencies have access to the NP2 system, and the information in the systems to which it provides access, based on their respective employees' need-to-know.

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 routine uses that permit this sharing and are compatible with the original purpose for the collection. These include Routine Uses (c) and (g).

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

Yes. Customer agencies to whom NBIB provides background investigations 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 NBIB are limited by the terms of their contracts.

Customer agencies using the NP2 System are also governed by EO 13467, as amended by EO 13764, which allows the agencies to release records within the agency and to record subject (if there is due process need). Each agency 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. Agencies may coordinate this activity with the NBIB 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.

The NP2 System uses audit logs to identify when a user logs in, where they go, what they do, when they do it.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in NP2 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.

Section 7. Redress

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

Certain information contained in NBIB records 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 NP2 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

NP2 System does not have the ability to notify the public and/or individual directly; however, 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: There is a risk that individuals may not have the opportunity to correct, access, or amend inaccurate information contained in NP2 System.

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?

Role-based access controls are employed to limit access to NP2 and its connected systems based on the need to know the information for the performance of the users' official duties. 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 background investigation information.

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

All OPM/NBIB employees and contractors that have access to the NP2 system are required to complete annual IT Security and Privacy Awareness training. In addition, NP2 system users are not authorized access to the system unless they have completed applicable Rules of Behavior required to perform the responsibilities being requested for the NP2 system.

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. The request for NP2 system access is initiated through designated supervisory channels of the potential user based upon their business responsibilities. NBIB access control officials evaluate and determine access to the system and the security office 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 MoUs and ISAs every three years for renewal or necessary adjustments. Any new access to the NP2 System will be evaluated by the appropriate NBIB personnel and documented in a MoU or ISA. New uses of the information are business decisions determined by the NBIB Information Technology Management Office (ITMO), in coordination with relevant stakeholders.

Responsible Officials

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