Privacy Impact Assessment
for the

Non-Field Work
(NFW)

April 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 the Non-Field Work (NFW) system is to facilitate data exchange electronically with external agencies / organization for NBIB. This Privacy Impact Assessment (PIA) is being conducted because the NFW 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

The United States Office Personnel Management (OPM) National Background Investigations Bureau (NBIB) conducts background investigations for Federal government agencies to use as the basis for suitability and security clearance determinations as required by Executive Orders and other rules and regulations. NBIB is responsible for most of the Federal government's background investigations, conducting millions of investigations each year on Federal applicants and employees, active military personnel, government contractors, and private sector employees in positions regulated by the government. In addition, NBIB has other responsibilities, including processing and providing informational reports within 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 through NBIB's Electronic Questionnaires 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). The PIPS is the primary system for the processing, storing and administration of background investigations on candidates for national security, public trust and non-sensitive positions within the Federal Government. In addition other relevant information is gathered (e.g., employment, credit, criminal history), and the investigators then produce various Reports of Investigation (ROI). The ROI is then reviewed for completeness and a general case review is conducted. The case is then closed and prepared for delivery. An electronic or printed paper file is then sent to the sponsoring agency, which makes the final decision/adjudication regarding the candidate's investigation. When the sponsoring agency makes its decision regarding the candidate's investigation, it returns the decision/adjudication to the PIPS system for record keeping.

System Overview

The NFW system acts as an automated batch or real- time data exchange broker between PIPS and external agencies and vendors (e.g., Social Security Administration (SSA), military organizations, law enforcement entities, and consumer reporting agencies). Its main function is to process automated National Agency Checks (NACs) that originate in PIPS and require verification or validation from one or more of various external agencies and vendors.

Once NACs are scheduled by PIPS, the NFW system pulls the information from the PIPS database that is required for the applicable agency or vendor to complete the NAC. NFW then sends a batch file electronically to the appropriate agency or vendor to obtain the information required for the investigation process. Once the information is received from the agency or vendor, the NFW system automatically updates the PIPS database with the information, sends any documents received to the OPM PIPS Imaging System (OPIS) as necessary, and provides reports to a small group of NBIB subject matter experts.

The NFW system has a simple user interface designed for a small group of authorized administrators to access through a restricted network from a highly secured operations center location. This interface allows the administrators to re-run the automated process if necessary, view error logs, or monitor and view the status of the processes running on the system. This is the only portion of the NFW system that allows for human interaction in the NFW processes.

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 NFW 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 NFW System Security Plan (SSP), Version 1.0, was completed as part of the system's Authority to Operate (ATO) on January 20, 2017. It was last updated to Version 3.0 in 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. Those records that are used, maintained, and disseminated through the NFW system are covered by General Records Schedule 5.2, Transitory and Intermediary Records.

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 NFW system is an automated backend system that does not collect information directly from individuals. However, the information brokered from PIPS to external agencies and vendors incorporates information that was collected subject to the PRA. These initial information collections do have assigned OMB control numbers and a list is included in the PIA for PIPS, available at www.opm.gov/privacy.

Section 2. Characterization of the Information

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

The information that the NFW system collects, uses, and disseminates information varies according to the NAC check, but can include the following information about the subject of the investigation as well as others associated with the subject's investigation: name, date of birth (DOB), place of birth (POB), address, Social Security number (SSN), other information relevant to identify the person being queried, and information obtained from the various vendors and agencies about the person being queried.

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

Identifying information about the subject of the NAC query is obtained, first, from PIPS through a system to system interface. The NFW system then sends that information to the appropriate NAC agency or vendor and

receives information back related to the particular query about the individual. Those agencies and vendors include but are not limited to: FBI, the Department of Defense (Defense Central Investigative Index (DCII)), Selective Service System, U.S. Citizenship and Immigration Services, Financial Crimes Enforcement Network (FINCEN), consumer reporting agencies (credit reports), Bureau of Vital Statistics (BVS), National Crime Information Center (NCIC), International Police (INTERPOL), and Social Security Administration (SSA). Additional sources of information include neighbors, educational and financial institutions, law enforcement entities, medical facilities, employees, and subject-provided references. That information is obtained through face-to-face interviews and written communication.

Investigative inquiries originate by electronic data exchange with specific entities in relation to obtaining or verifying information regarding the individual's activities, such as employment, residence, education history, criminal history, and other personal information.

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. The NFW system obtains information about individuals from various consumer reporting agencies and publicly available NAC repositories, including the national consumer reporting agencies, and updates the PIPS database base with that information. The use of the 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 investigation 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.

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 NBIB case analysts reviewing the information from NFW and validating applicant information by comparing data, such as name, social security number, and date of birth in the PIPS database.

Privacy Risk: There is a risk that incorrect information could be obtained from PIPS by the NFW system, resulting in inaccurate NACs being returned from the various agencies and vendors.

Mitigation: This risk is partially mitigated by incorporating reviews by NBIB case analysts who confirm subject information by comparing data, such as name, social security number, and date of birth in the PIPS database.

Section 3. Uses of the Information

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

The NFW system is a backend system that automatically brokers data exchanges between PIPS and external agencies or vendors to process NACs. The system only administers the passing of the information from one system to another (internally and external to NBIB). Information brokered through NFW is passed to agency adjudicators to determine an individual's suitability

and/or fitness for Federal employment, a position of trust with the Federal government, and/or for eligibility and access determinations.

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 NFW system does not use tools, programs, or technology to predict patterns or anomalies.

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

The NFW system has a simple user interface designed for a small group of authorized administrators to access through a restricted network from a highly secured operations center location. This interface allows the administrators to re-run the automated process if necessary, view error logs, or monitor and view the status of the processes running on the system. This is the only portion of the NFW system that allows for human interaction in the NFW processes. There are no other programs and offices with assigned roles and responsibilities within the system, though authorized NBIB personnel and contractors have need-to-know access to investigation information, including information that passes through the NFW system.

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

Privacy Risk: There is a risk that authorized individuals may access the system for an unauthorized purpose or that unauthorized individuals may obtain access to the system.

Mitigation: This risk is mitigated by permitting access to the NFW system to only a small number of administrators, based on their need-to-know, and through use of 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.

The NFW system does not provide direct notice to individuals regarding its collection and use of background investigation information. 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 will not receive adequate notice concerning how their information is being used in NFW.

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 NFW specifically, it does provide information concerning how their information will be used. In addition, notification is provided through publication of this PIA.

Section 5. Data Retention by the project

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

The data sets created by the NFW system from information in the PIPS database are stored for up to 30 days to facilitate reprocessing the NACs if necessary. The information obtained from the NAC agencies and vendors are also stored up to 30 days for troubleshooting, as necessary. After 30 days all information including NFW generated reports are deleted from the system.

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 adhering to the business rule regarding retention of records in NFW. The NFW system is designed to delete all the information obtained from PIPS, NAC agencies, vendors, and self-generated reports in 30 days.

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. The nature of the NFW system is that it shares information with the NAC agencies and vendors in order to gather relevant information required to conduct a background investigation.

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. The OPM/CENTRAL 9 SORN contains the following routine uses specific to that permit this sharing and are compatible with the original purpose for the collection: 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.

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

Yes. NBIB has MOUs with the agencies who conduct NACs for the background investigation process that limit the use and re-dissemination of information. Use and re-dissemination of information by vendors conducting NACs are limited by the terms of their contracts

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

The NFW system audit logs track when and where the NAC data was sent and received electronically.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in NFW will be exchanged 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 limiting use and re-dissemination in MOUs and contracts and through the review of audit logs to determine appropriate information release.

Section 7. Redress

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

The NFW system is an internal NBIB backend automated system. Individuals have no access to the information in the NFW system. In addition, certain information contained in NBIB systems 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?

The NFW system is an internal NBIB backend automated system. Individuals have no access to the information in the NFW system. In addition, certain information contained in the NBIB system 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 generally concerning the procedures for requesting the amendment of records on the NBIB public website, https://nbib.opm.gov/foia-privacy-acts/requesting-and-amending-myrecords/#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 obtained about them in the investigation process.

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 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?

Only a limited group of NFW system administrators have access to the system in order to perform their duties in managing and using the system. Role-based access controls are employed to limit the access of information, based on the need to know the information for the performance of their official duties. The NFW system also employs processes to enforce separation of duties, prevent unauthorized disclosure, and 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 coordination with the OPM Security and Privacy Policies Handbook Version 3, March 31, 2011 and the updated addendum policies.

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

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

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

The NFW system has a simple user interface designed for a small group of authorized administrators to access through a restricted network from a highly secured operations center location. This interface allows the administrators to re-run the automated process if necessary, view error logs, or monitor and view the status of the processes running on the system. This is the only portion of the NFW system that allows for human interaction in the NFW processes. The request for NFW 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 every three years for renewal or necessary adjustments. Any new access to the NFW system will be evaluated by the appropriate NBIB personnel. 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