Privacy Impact Assessment
for the

Field Work System
(FWS)

February 15, 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 (U.S.) 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 Field Work System (FWS) is to provide special access for NBIB investigators, record checkers and support staff comprised of both federal employees and contractors located throughout the world, the ability to read, add, and update investigative data. This Privacy Impact Assessment (PIA) is being conducted because the FWS contains Personally Identifiable Information (PII) about applicants 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 Field Work System (FWS) is a client application that is designed to assist OPM field agents and investigators who conduct interviews as part of the background investigation process. These include approximately 7750 federal and contractor NBIB investigators, along with an additional 40 support personnel, located throughout the world. FWS is essentially an easy to use graphical interface to PIPS that provides users the ability to work while disconnected from the OPM network. The core functionality of FWS is to provide a view of assigned investigative tasks, the ability to edit investigative case messages, and the ability to write reports of investigations (ROIs). The system also provides map views and directions for investigative tasks and interviewees, and enables users to add items to investigative tasks, transmit ROIs, schedule extensions, and send case messages to federal and contract investigators. Users launch the FWS application from their Windows desktop on either contractor or OPM owned devices, which include laptops, desktops, or Windows to Go USB sticks and can only access the information related to cases specifically assigned to them. FWS data is stored in a local database for off-line availability and any changes or updates made by the investigator are synchronized the next time the system is

connected to PIPS. Once a case closure message has been issued for a closed case in PIPs (30 days after a case has closed), the case data is purged from the local FWS database. All of the information in FWS is information that is transferred from PIPS or entered by the investigator for ultimate inclusion in PIPS. FWS does not contain any additional unique information.

The FWS application can operate in three modes as described below:

Full System Functionality: In this mode the investigator is working as if they were on the OPM network with all the functionality that it provides. Investigators need to connect to this mode first to download their case assignments. At this stage they are able to acquire information about the applicants that they will be investigating.

On-Line-Disconnected from PIPS: In this mode the investigator has access to network functionality such as maps and directions features to help in scheduling site visits to the applicants that they will be interviewing. This feature allows them to schedule several visits in the same geographical location so that they can save time going between different applicants. This information is only available after the investigator has connected with full system functionality and downloaded their assignments.

Off Line: In this mode, the investigator is not connected to the network and can work only on what they have on their laptop. In this mode, the investigator can take notes after their appointment with applicants or others whom they are interviewing on behalf of the applicants investigation, which will be included in Reports of Investigation that are transmitted to PIPS when the investigator is working in Full System Functionality mode.

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 FWS 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 FWS System Security Plan (SSP), Version 1.0, was completed as part of the system's Authorization to Operate (ATO) on January 20, 2017. It was last updated to Version 3.0 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, 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.

FWS uses data transmitted to the system via the Personnel Investigations Processing System (PIPS). Investigators then collect additional information and enter it into FWS. There are no applicable OMB control numbers specific to the collection of information by FWS. However, the information obtained

from PIPS incorporates information that individuals record on various forms. 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.

WS collects, uses, disseminates, and 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 and obtained in the background investigation process. In addition, FWS may contain information about individuals other than the subject of the background investigation, such as their spouse/cohabitant, close relatives, employers, doctors and other medical personnel, neighbors, and other individuals that the applicant identifies or who are identified by the investigator during the course of the investigation. FWS also may contains other historical information about the applicant that is obtained 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 FWS comes from two sources, PIPS and the investigator. Information is received from PIPS via a secure connection and from the investigators via data entry into FWS templates after conducting interviews.

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. FWS uses BING Maps to identify the geographic location of individuals that the investigator needs to interview. This helps in scheduling interviews with all parties at a single location so that the investigator does not need to re-visit the same location multiple times.

2.4. Discuss how accuracy of the data is ensured.

FWS performs field validations, including address checks against commercially available maps, date fields checks, enforces required fields, limits the number of characters, and provides drop-down fields to limit input errors. Information submitted by FWS is validated by PIPS. If there are anomalies, the ROI is returned to the investigator in the FWS for further correction.

Every effort is made by the investigators to verify any inconclusive information that they acquire during the course of the investigation. Interviewees are asked to provide corroborating information, names of other individuals who could be interviewed to corroborate the information that they provide. The investigators also utilize public records as well as information in PIPS and other government and commercial systems.

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 and because the system relies on information from other sources, it is possible that incorrect information could be included in their system.

Mitigation: This risk is mitigated by the investigator validating the information obtained from the PIPS and through FWS's field validations, enforcement of required fields, drop down menus, and other mechanisms described in Section 2.4.

In addition, individuals are required to certify that the information they provide at the initial point of collection is complete and accurate in NBIB's Electronic Questionnaire for Investigations Processing (e-QIP), a secure website designed to automate the security questionnaires used to process federal background investigations of the applicant.

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 of the individual being investigated.

Mitigation: This risk is mitigated through training investigators on the proper use and meaning of the information obtained during an investigation. In addition, authorized users of FWS sign an agreement that requires them to properly use the information in the system.

Section 3. Uses of the Information

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

FWS is used by investigators to help them keep track of information collected by them during the investigative process. The investigator is then able to decide if the information collected is complete or not, and has the ability to note that more information is needed if necessary, including the identification of potential sources of the information. Once the investigator completes their investigation work, information collected by FWS is uploaded to the PIPS mainframe database to be used by NBIB staff to generate reports for the agency requesting the investigation of the applicant. A local database server is used to hold data that investigators work on or information retrieved from PIPS as needed by the investigators to perform a proper investigation. Data is stored in the local database until the case is closed and the investigator syncs in online mode with the PIPS database..

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 FWS does not use any tools, programs, or other technology to conduct electronic searches, queries, or analysis of the local database to discloser or locate a predictive pattern or anomaly.

FWS utilizes Bing Maps to help investigators locate where in-person interviews are to be held. This allows investigators to schedule multiple interviews at proximate locations.

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

The majority of FWS users are Federal and contract investigators who use FWS to manage their work assignments and enter investigation information. Record searchers or investigative assistants (IAs) use FWS to perform record searches. NBIB support personnel, including technical support and trainers, use FWS in support of the investigators in the field..

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

Privacy Risk: There is a risk that authorized users may access information for an unauthorized purpose and use in a manner inconsistent with the purpose for which it was collected.

Mitigation: This risk is mitigated through training investigators on the appropriate use of information and 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 received Annual Security and Privacy Awareness Training.

In addition, a strongly worded notice is provided to users when they open the FWS application, explaining the expectations, the risks and the consequences.

There are also multiple layers of physical and IT security protections that are used to safeguard the data. Physical security on the premises ensures that only authorized individuals have access to the building. Layered firewalls and data encryption methods ensure the data can only be accessed by individuals authorized by NBIB Access Control.

Privacy Risk: 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 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.

FWS 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.

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

The standard forms in FWS contain Privacy Act Statements, and inform the applicants that providing the information is voluntary, so individuals may decline to provide information or opt out of the project. However, if an individual does not provide each item of requested information, the standard form will not be submitted and the background investigation cannot be processed.

Applicants do not have the ability, once they have agreed to the background investigation, to consent to some uses of their information and decline to consent to other uses. The exception to this is the SF86 Medical Release authorization, which is valid for one 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 FWS.

Mitigation: This risk is mitigated by the providing individuals with a Privacy Act statement at the initial points of information collection and at the beginning of an in person interview. While that statement does not explain the system specifically, it does provide information concerning how their information will be used. In addition, notification specifically about this system 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 records in FWS are subject to the retention schedule referenced in Section 1.4. They are stored in the local database until the case is closed and the investigator syncs in online mode with the PIPS database.

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. 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.

Contractor investigators have access to FWS and the information it contains but otherwise information is not shared directly from FWS outside of OPM.

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

Contractor investigators have access to FWS and the information it contains but otherwise information is not shared directly from FWS outside of OPM. The contractor access is contemplated in Routine Use (g) in the OPM/Central 9 SORN: "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?

Contractor investigators who have access to FWS and the information contained therein are required to adhere to the terms of their contract regarding use and dissemination of the information they access.

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

Contractors obtain access based on their need to know the information contained in FWS. A contractor's access to information can be determined through role-based access controls and system audits.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in FWS 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 through training investigators regarding the appropriate use and handling of the information in FWS and through the use of user access controls based on an individual's need to know.

Section 7. Redress

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

Individuals from the public have no access to the information in the FWS but may generally request access to their investigation information.

Certain information contained in the NBIB systems 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 the NBIB system and covered by the OPM/CENTRAL 9 SORN has been exempted from the access and amendment requirements in the Privacy Act. Individuals may seek to correct non-exempt information by contacting FOI/PA, Office of Personnel Management, National Background Investigations Bureau, P.O. Box 618, 1137 Branchton Road, Boyers, PA, 16018-0618, in writing. Individuals may submit their request by using form INV100 Freedom of Information, Privacy Act Record Request Form or by sending the following information: full name, date of birth, place of birth, SSN, precise identification of the records to be amended, , a statement about and evidence supporting the reasons for the request, including all available information substantiating the request; mailing address and email address to which correspondence should be sent, a signed and notarized statement or an unsworn statement declaring that the information submitted is true, and copies of two identity documents.

7.3. How does the project notify individuals about the

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

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have the opportunity to access or amend their information.

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?

The FWS 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. FWS enforces separation of duties, preventing unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system.

All customer agencies are bound by MoUs and ISAs that document the appropriate access, use, and dissemination of investigation-related information. In addition, this document and the procedures contained herein are reviewed 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 having access to the FWS are required to complete the annual IT Security and Privacy Awareness training. In addition, the FWS users are not authorized access to the system, unless they have completed applicable investigator training.

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

Investigators are selected and trained specifically for the NBIB mission. Access is handled through NBIB security offices, utilizing a Resource Access Control Facility (RACF). Users must be in the RACF group in order to gain access to the FWS.

Access to any part of the system is approved specifically for, and limited to, users who have an official need to know the information for the performance of their investigative duties. NBIB's access control officials 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 the MoUs and ISAs every three years for renewal and makes any necessary adjustments. New uses of the information are business decisions determined by the NBIB Information Technology Management Office, in coordination with relevant stakeholders.

Responsible Officials

Charles S. Phalen, Director
National Background Investigation Bureau

Approval Signature

Signed Copy on File with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer