Privacy Impact Assessment
for the

Fingerprint Transaction System (FTS)

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 the Fingerprint Transaction System (FTS) is to provide a secure means for approved agencies to submit electronic or hard copy fingerprint images to the Federal Bureau of Investigation's Criminal Justice Information Services via NBIB's Federal Investigations Processing Center (FIPC). This Privacy Impact Assessment (PIA) is being conducted because FTS contains Personally Identifiable Information (PII) about candidates who are undergoing a background investigation.

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 Fingerprint Transaction System (FTS), the subject of this PIA, handles fingerprint checks for the Federal background investigations. FTS provides federal agencies the ability to submit fingerprint searches electronically through NBIB to the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigations (FBI). The Card Scan Center (CSC) receives and converts fingerprint hard cards into FBI's Electronic Fingerprint Transmissions Specification (EFTS) before transmission to CJIS. FTS utilizes a dedicated T-1 secure connection called the CJIS WAN; this connection sends and receives updated fingerprint results obtained by the FBI-CJIS Integrated Automated Fingerprint Identification System (IAFIS). The search results of the fingerprint images are sent back to FTS and are provided to other NBIB systems that contribute to the overall investigative process. The investigative data associated with those fingerprints is also stored in the Personal Investigation Processing System (PIPS) database.

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 FTS 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 FTS System Security Plan (SSP), Version 1.2 November 25, 2016, was completed as part of the system's Authorization to Operate (ATO) on January 20, 2017. It was last updated to Version 1.3 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) Input Records, Output Records and Electronic Copies, Records Schedule Number DAA-0478-2012-0003.

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.

FTS collects the fingerprints via the SF-87 and FD-258 forms. The Office of Management and Budget (OMB) control numbers for the initial collections of fingerprint information are as follows:

Form Number	Form Name	OMB Number
SF-87	Fingerprint Chart	OMB No. 3206-0150

Form Number	Form Name	OMB Number
FD-258	Standard Fingerprint Form	OMB No. 1110-0046

Section 2. Characterization of the Information

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

FTS collects, uses, disseminates, and maintains the following Personally Identifiable Information (PII): name, AKA, Social Security number, date of birth, place of birth, hair color, eye color, weight, height, sex and race. It also contains the criminal record responses from FBI-CJIS and applicant's electronic fingerprint images.

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

Applicants provide information in support of their own personal background investigation, which is a prerequisite for federal employment. Live scanners are used to collect and digitize an applicant's fingerprints with their PII. These digitized fingerprints, along with the PII for certain types of fingerprint submissions, are submitted to and stored within FTS.

In addition to applicant data submitted electronically to FTS, information from two other systems is used and stored within FTS: 1) Existing PII information and system responses associated with an applicant in PIPS that is sent to or requested by FTS ,and 2) Criminal history records, non-ident, and error responses from the FBI-CJIS.

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

No. The FTS does not use information from commercial or publicly available data sources.

2.4. Discuss how accuracy of the data is ensured.

No. The FTS does not use information from commercial or publicly available data sources.

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

Privacy Risk: There is a risk that subject information in the system may not be accurate.

Mitigation: This risk is mitigated by the validations described in section 2.4. The risk is also mitigated by collecting data elements sufficient to distinguish a candidate from other individuals. In addition, in cases where the print quality is unacceptable and the FBI cannot return a valid result, an additional fingerprint submission may be sent to FBI-CJIS to obtain a valid result.

Section 3. Uses of the Information

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

FTS provides the biometric capability to the NBIB background investigative process. FTS provides electronic fingerprint images received from external agencies to the FBI-CJIS to perform a criminal history check. It also converts fingerprint hard cards into electronic images using site-to-site Virtual Private Network (VPN), dial up, communications server or Connect-Direct via the NBIB's Federal Investigations Processing Center (FIPC). The results of the criminal history check, including any existing arrest records, are sent back to FTS. The investigative data associated with the fingerprints is also stored in 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, FTS 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 support contractors in NBIB who have a need for the information in the performance of their job duties have access to FTS and the information contained therein.

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

Privacy Risk: There is a risk that PII in the system may be accessed or used inappropriately or in a manner not consistent with the purpose for which it was collected.

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 by the system will 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 also 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 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.

FTS is a NBIB internal system not accessible by the public and/or individuals, therefore, notice is not given by the system. However, subjects of investigation are provided notice and the ability to consent, in the form of a Privacy Act statement on the SF-87 or the FD-258, at the original point of the information collection.

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 informed by the Privacy Act statement that submission of the information is voluntary, however, failure to provide their information will not permit the agency to complete the background investigation.

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: The risk is partially mitigated by the provision of the Privacy Act Statement on the SF-87 and FD-258. The Privacy Act Statement informs the individual on the uses of the information. While that statement does not explain the system specifically, it does provide information concerning how their information will be used. It is not clear whether applicants who submit their fingerprints via a live scanner and not via one of the referenced forms receive a Privacy Act statement and, for those individuals, notice is provided only 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.

FTS follows 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. Records may be maintained only as long as the individual remains of interest to the agency for the purposes defined in the Central 9 SORN (e.g. suitability, security, credentialing purposes). Upon separation or when the individual is no longer of interest to the agency, the agency must dispose of any/all background investigation records.

For the records in FTS where there is a site-site connection and the system accepts electronic submissions (i.e. LiveScans), NARA Disposition Authority DAA-0478-2012-0003-0001 applies. For these records, once received in NBIB and the information is transmitted to CJIS, they must be deleted when data has been imported to the master file or when no longer required to support reconstruction of, or serve as backup to, master file or database (whichever is later). These records are considered inputs received from other agencies as part of interagency agreements and are therefore excluded from GRS 4.3 (Input Records, Output Records and Electronic Copies), item 020 (DAA-GRS-2013-0001-0004)

All other records containing subject fingerprints, demographic data and results of Identification check from FBI and CJIS responses are considered temporary and must be destroyed or deleted 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use (Disposition Authority - DAA-GRS2017-0006-0024). Records that are created to support favorable eligibility determination, periodic reinvestigations, or to implement a continuous evaluation program that include questionnaires, summaries of reports, and documentation of agency adjudication processes and final determinations will be destroyed 5 years after the employee or contractor relationship ends, but longer retention is authorized if required for business use (Disposition Authority - DAA-GRS2017-00060025). This includes records of applicants issued clearances and those not hired. This does not include investigative reports covered under Disposition Authorities DAA-GRS2017-0006-0022 and DAA-GRS2017-00060023.

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 staffs 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.

FTS shares records and information with the FBI for the purpose of obtaining criminal history record information. This information is transmitted through a secure connection.

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 that permit this sharing and are compatible with the original purpose for the collection:

(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.

(l) To provide criminal history record information to the FBI, to help ensure the accuracy and completeness of FBI and OPM records.

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

Customer agencies to whom NBIB provides background investigation information are limited in their use and re-dissemination of the information, as outlined in MoU and ISA. Use and re-dissemination of information by contractors conducting the background investigations for NBIB are limited by the terms of their contracts. The information that NBIB submits to FBI-CJIS through FTS is retained in accordance with FBI's records retention schedule and used in accordance with applicable law and policy.

Entities using FTS and other 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.

FTS tracks the submission of fingerprints to the FBI via a system log.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in FTS 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 individuals with access to the system on appropriate use of the information and through establishing secure connections and role based access controls so that only authorized individuals and entities can obtain the information in the system.

Section 7. Redress

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

Certain information contained in FTS 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 FTS 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 correct, access, or amend inaccurate information maintained by other agencies and shared to FTS.

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 the access of information by users and administrators based on the need to know the information for the performance of their official duties. Strict adherence to access control policies is automatically enforced by the system.

This document and the procedures contained herein are reviewed regularly by the relevant OPM and NBIB offices 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 FTS are required to complete the annual IT Security and Privacy Awareness training. The FTS system users are not authorized access to the system unless they have completed applicable training required to perform the responsibilities being requested for the FTS 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?

FTS has associated information technology roles that limit the capabilities and access to data. 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 office grants access to the system based on a need to know and business role. Access to FTS is internal only to NBIB and the supporting contracting staff.

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 and makes any necessary adjustments. Any new access to, or use of information in, FTS will be evaluated by the appropriate NBIB personnel.

Responsible Officials

Charles S. Phalen, Director
National Backgroound Investigation Bureau

Approval Signature

Signed Copy on File with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer