Department of the Treasury
BUREAU OF ENGRAVING AND PRINTING

Finger Print Scanning System (FPSS)

February 3, 2015

B. System Application/General Information

1. **Does this system contain any PII? [ ] No [X] Yes**

2. **What is the purpose of the system/application?**

   The U.S. Office of Personnel Management (OPM) provides a reimbursable service called the Fingerprint Transaction System (FTS) to electronically accept and process Electronic Special Agreement Checks (e-SACs). Federal agencies interface with the OPM FTS with an optical Finger Print Scanning System (FPSS).

   The Office of Security - Personnel Security Division (DCF) and the Office of Manufacturing Support-Security Division, Personnel Security Branch (WCF) use the FPSS to capture digitally the fingerprints of contractors, employees, and applicants who will be working at BEP. In addition, this system also records other PII about every individual whose fingerprints are captured by the system. The fingerprints and PII are transmitted electronically to OPM. OPM then interacts with the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigations (FBI) to obtain the requested information. OPM provides the resulting data to the BEP on a secure portal and by mail (United States Postal Service (USPS) or United Parcel Service (UPS) signature required). The data generated by OPM is not stored in the FPSS. The data is printed and filed in the individual's security folder and stored in a secure safe or Lektriever filing cabinet.

3. **What legal authority authorizes the purchase or development of this system/application?**

   31 U.S.C. § 321, 44 U.S.C. § 3544, 5 C.F.R. § 731, 5 C.F.R. § 732, Executive Order 10450 as amended, 18 Fed. Reg. 2489 (April 27, 1953), Executive Order 12968 as amended, 60 Fed. Reg. 40245 (August 7, 1995), and Homeland Security Presidential Directive 12 (HSPD-12).

4. **Under which SORN does the system operate? (Provide name and number)**

   Treasury/BEP .021 Investigative Files, 73 Fed. Reg. 22604 (April 16, 2013)
   Treasury .007 Personnel Security System, 79 Fed. Reg. 183 (January 2, 2014)

C. Data in the System

1. **What categories of individuals are covered in the system? (e.g., employees, contractors, taxpayers, other)**

   The system covers contractors, employees, and applicants.

2. **What are the sources of information in the system?**

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other sources?

The individual supplies all information in the system. The individual can also supply a state issued driver license. The driver license is scanned through a card reader attached to the FPSS and PII is populated into the record.

b. What Federal agencies are providing data for use in the system?

There are no federal agencies providing data for this system.

c. What state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for us in the system?

The individual only provides the data in this system. There are no state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for this system.

d. From what other third party sources will data be collected?

Only the individual provides data. The individual can supply a state issued driver license that is scanned through a card reader allowing the PII to be populated into the data fields.

e. What information will be collected from employees, government contractors and consultants, and the public?

The following information is collected from the individual:

- Name (Last, First Middle, Suffix);
- Aliases;
- Date of Birth;
- Sex;
- Race;
- Height;
- Weight;
- Eye Color;
- Hair Color;
- Place of Birth;
- Fingerprints;
- Residence;
- Employer name and address
- Occupation
- Social Security Number;
- Country of Citizenship;

- Transaction Date;
- Amputated Finger Indication; and
- Bandaged Finger Indication.

3. **Accuracy, Timeliness, and Reliability**

   a. **How is data collected from sources other than from Treasury records going to be verified for accuracy?**

   No data is collected from sources other than the individual.

   b. **Is completeness required? [ ] No [X] Yes**

   c. **What steps or procedures are taken to ensure the data is current and not out-of-date?**

   The record is edited as needed if subsequent prints are required from the individual.

   d. **Are the data elements described in detail and documented? [ ] No [X] Yes**

   In the Fed Submit User's Guide.

D. Attributes of the Data

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

   Yes. This information is used to conduct background investigations of all applicants, employees, and contractors to ensure that these individuals meet established suitability and security standards.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? [] No[X] Yes**

   FPSS does not generate or derive any new data. However, the query generated by FPSS and sent to OPM may generate new data. The data generated by OPM is not stored in the FPSS. BEP accesses the data generated by OPM from the secure portal and the data is printed. OPM also sends the data by mail (United States Postal Service (USPS) or United Parcel Service (UPS) signature required). The data is filed in the individual's security folder and stored in a secure safe or Lektriever filing cabinet.

3. **Will the new data be placed in the individual's record? [] No [X] Yes**

The data generated by OPM from the secure portal and delivered by mail will be filed in the individual's security folder and then stored in a secure safe or Lektriever filing cabinet.

4. **Can the system make determinations about employees/members of the public that would not be possible without the new data?**

The FPSS cannot make any determinations. However, BEP's Personnel Security Division and Personnel Security Branch use the data provided by OPM to make any suitability determination that would not have been possible otherwise.

5. **How will the new data be verified for relevance and accuracy?**

BEP's Personnel Security Division and Personnel Security Branch personnel verify the data provided by OPM with the specific individual involved.

6. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

FPSS is not consolidating data. However, the data sent back from OPM represents a consolidation of data. The controls to protect this data consolidation are not a part of the FPSS.

7. **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

FPSS provides a stimulus, the request for background information from OPM that OPM acts on. OPM generates a request to the FBI for data and then generates a report using the FBI data which is presented for BEP's use. FPSS has adequate controls, both physical and logical, to safeguard unauthorized access to the FPSS component of this process consolidation. BEP's Personnel Security Division and Personnel Security Branch have physical access controls to protect the data provided by OPM. This PIA does not address the controls present at OPM or the FBI.

8. **How will the data be retrieved? Is the data retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

The data is retrieved by name or transaction control number only.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The purpose of this system is to send a digitized fingerprint card for a query on a specific individual to OPM for background investigation action by the FBI. The mechanics of how this data is used once it leaves the FTS are not covered under this PIA.

The FPSS provides a wide variety of reporting capabilities including:

- Open Transactions by Date Range;
- Unsubmitted Transactions;
- Open Transactions;
- Completed Transactions;
- Submission Log Report;
- Operator Activity Report;
- Ident Hit Report (Check); and
- False Name Report (Check).

These reports are used primarily to track the status and health of the data submission and result process. While the reports may contain elements of PII, such as an individual's name, these reports are not printed or stored in an individual's file.

E. Maintenance and Administrative Controls

1. **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   The system operates at the DCF and WCF. These systems do not share data.

2. **What are the retention periods of data in the system?**

   Records are retained in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) No. 18 (NC1-GRS-80-1, items 22a and 21.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

   Paper records beyond their retention period are destroyed by shredding or burning. Electronic records beyond their retention period are electronically erased using accepted techniques. Reports generated that are not included in the case files are retained in accordance with NARA GRS No. 18 (NC1-GRS-80-1 item 21).

   The procedures used to facilitate this process are documented in BEP Circular No. 80-05, Records Management Program (2006); BEP Circular No. 80-05.3, Records Storage (2007); and BEP Circular No. 80-05.4, Policies and Procedures for Electronic Records and Email (2006).

4. **Is the system using technology in ways the office or bureau has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, explain.**

No.

5. **How does the use of this technology affect public/employee privacy?**

   The system collects information that uniquely identifies an individual. This data includes an individual's fingerprints, one of the very few unique identifiers. This data is placed in a BEP database and shared with the OPM and the FBI. An individual refusing to provide the information would prevent the BEP from obtaining the required information to complete a background investigation. A satisfactory background investigation is required to obtain a position at the BEP.

6. **Will the system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   The function of this system is to provide OPM with information needed to perform background investigations. Therefore, the identifiers in this system could all be used to identify an individual. However, the system has no capability to locate or monitor an individual.

7. **What kind of information is collected as a function of the monitoring of individuals?**

   The system has no capability to locate or monitor an individual.

8. **What controls will be used to prevent unauthorized monitoring?**

   The system has no capability to locate or monitor an individual.

9. **Under which SORN does the system operate? (Provide name and number)**

   Treasury/BEP .021 Investigative Files, 73 Fed. Reg. 22604 (April 16, 2013)
   Treasury .007 Personnel Security System, 79 Fed. Reg. 183 (January 2, 2014)

10. **If the system is being modified, will the SORN require amendment or revision? Explain.**

    A new system is being purchased to replace the existing system. The system functionality will not change and therefore the SORN will not require modification.

F. <u>Access to Data</u>

1. **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others).**

Federal employees of the BEP will have access to the data in the system. The data is sent to OPM as part of the background investigation process. OPM then shares the data with the FBI as part of the BI request process.

2. **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

   User access to this data is determined by job descriptions and the user's roles and responsibilities.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   Users of this system will have access to all the data in the system. This information is intrinsic to their job functions.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? List procedures and training materials.**

   The room in which the system is located, is physically secured. Staff must use their badges in order to enter the room. Additionally, all users must authenticate to the machine via a network login. Users must then authenticate to the FPSS via a login and password unique to the user. Reports can be generated to display the name of the user and the record they have submitted. User permissions restrict what a user can do once logged into the FPSS. Only system administrators have full access to the system.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

   A vendor called Mentalix, Inc. provides this system. The vendor assists with maintenance but does not have access to the data in the system. Additionally, a BEP employee is always present when the vendor is accessing the machine, which hosts the system.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

   Yes. The data collected by this system is transmitted to the OPM so that the FBI can perform a background investigation.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   Chief, Office of Security
   Manager, Security Division, WCF

8. **Will other agencies share data or have access to the data in this system?**

[X] Federal **[ ] State** **[ ] Local** **[] Other**

The data collected by this system is transmitted to the OPM. OPM then formats the data and sends it to Criminal Justice Information Services (CJIS) Division of the FBI to obtain the requested background information.

9. How will the data be used by the other agency?

Fingerprints are sent to OPM for processing. OPM then sends these fingerprints to the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigations (FBI) for a background check. Once the FBI has the results, the information is sent back to OPM and posted on an OPM Secure Portal. OPM also sends the results via USPS or UPS. BEP personnel log onto the OPM secure portal in order to view and print the results. These results are never sent to the BEP FPSS.

10. Who is responsible for assuring proper use of the data?

Chief, Office of Security
Manager, Security Division, WCF