Automated Electronic Fingerprinting (AEF) – Privacy Impact Assessment

PIA Date – Oct. 2, 2009

System Overview

Automated Electronic Fingerprint (AEF) is used to scan and transfer fingerprint cards to the Federal Bureau of Investigation (FBI) for performing criminal background checks for e–File applications. AEF is utilized to dramatically reduce the time and money required for the FBI to process the fingerprints for each individual. The system interfaces with the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

Systems of Records Notice (SORN):

- IRS 22.062--Electronic Filing Records.
- IRS 36.003--General Personnel and Payroll Records
- IRS 34.021--Personnel Security Investigation, National Background Center (NBIC)

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer
   - Last Name
   - First Name
   - Middle Name (or NMN)
   - Gender
   - Race
   - Height
   - Weight
   - Eye Color
   - Hair Color
   - Place of Birth
   - Date of Birth
   - Date Fingerprinted
   - OCA Number (OCA is a Federal Bureau of Investigation (FBI)/National Criminal Investigation Center (NCIC) acronym meaning "originating agency's case number." This number is unique to one person/one arrest)
   - Transaction Control Reference (IAFIS Response Code)

B. Employee
   - SEID – used in place of a User ID and password

C. Audit Trail
   - Name
   - SSN
   - Barcode ID (each card has this ID attached to it so that any transactions that occur to the card will contain this ID)
   - Event (any transaction or error)
   - Current State- the state of the transaction that is happening (e.g., complete, error, edit, search, etc…)

D. Other
- The email message that is received from the FBI that states the results of the criminal background investigation will be used within the AEF processing environment. This email can be either one of two types. Type 1: an email notifying AEF that there was “no information found” on the individual. Type 2: an email would notify the AEF system of any criminal history recovered through the background investigation. This information may include: type of arrest and date, criminal charges and dates incurred, name and location of police department related to incidents.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS
- The FD–258 fingerprint card is provided by the IRS to taxpayers and police departments for the taxpayers to complete. This card and its corresponding information is the only source of data that is used throughout the criminal background investigation process.
- AEF validates the SSN by checking the SSN against the Third Party Data Store (TPDS). TPDS is a component of E–Services.

B. Taxpayer
- When completing the fingerprint card the taxpayer provides the following information to the IRS:
  - Signature
  - Name
  - Place of Residence
  - Employer
  - Employer Address
  - Aliases
  - Citizenship
  - Gender
  - Race
  - Height
  - Weight
  - Eye Color
  - Hair Color
  - Place of Birth
  - Date of Birth
  - Prior Military Service (if applicable)

C. Other Federal Agencies
- The Federal Bureau of Investigation (FBI) will be providing data for use within the AEF system through providing email messages that provide the results of background investigations.

3. Is each data item required for the business purpose of the system? Explain.

Yes. The use of the AEF technology is both relevant and necessary to the purpose for which the AEF implementation was designed. All information used within the AEF processing environment captured on the FD–258 fingerprint card is necessary for the business purpose of the system.

4. How will each data item be verified for accuracy, timeliness, and completeness?

There will be no additional data collected from any source other than the applicant’s FD–258 fingerprint card. Currently, there is a manual process to confirm and compare data on the fingerprint

card with data in the Third Party Data Store system (TPDS), which is an e-services subsystem for data records of registrants. This check is done to verify that name, address, and SSN are accurate.

5. Is there another source for the data? Explain how that source is or is not used.
No. There will be no additional data collected from any source other than the applicant's FD–258 fingerprint card.

6. Generally, how will data be retrieved by the user?
Viewing and retrieving information in AEF can be done in two ways. 1) An AEF user can query via Cogent Graphic User Interface (GUI) functionality using name, SSN, or barcode assigned to each fingerprint card. 2) An image of the actual fingerprint card will be displayed, and an AEF user can read the card for information.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
The Data/Fingerprint card image is retrievable by querying for name, SSN, or fingerprint card barcode via Cogent GUI functionality.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
All AEF users, managers, system administrators, and database administrators that have a need–to–know will access AEF data via Role-based Access Controls (RBAC).
The following chart details the roles and permissions of AEF users.

Role: Clerical, Tax Examiner (TE) Assistors, Leads, Managers
Permission: Document Scanner – Start and stop the Epson Scanner.

Role: Clerical, Tax Examiner (TE) Assistors, Leads, and Managers
Permission: Transaction Manager – Perform data entry for fingerprint submissions, edit transactions, and review search results.

Role: Leads, Managers
Permission: Archive Manager – View previously archived transactions.

Role: Leads, Managers
Permission: Lock Manager – Unlock transactions that have been locked.

Role: Leads, Managers
Permission: Report Manager – Generate and print identified reports.

Role: Leads, Managers
Permission: Barcode Printer – Print barcode label.

Role: Database Administrator
Permission: Provides MS SQL Server Assistance/ Generate reports/ create ad hoc reports.

Role: System Administrator
Permission: System level access in order to maintain the application and underlying infrastructure.

9. How is access to the data by a user determined and by whom?
AEF user access to the system is reviewed by AEF managers using Role-based Access Controls (RBACs) and authorized via the Online 5081 approval process.

Note: Contractors do not have access to the AEF system.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes. AEF validates the SSN by checking the SSN against the Third Party Data Store (TPDS). This check is not via manual comparison of the data, and is done electronically. TPDS is a component of E–Services.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

E-Services – Third Party Data Store (TPDS)

- Certification & Accreditation (C&A) – March 11, 2008
- Privacy Impact Assessment (PIA) – November 26, 2007

12. Will other agencies provide, receive, or share data in any form with this system?
AEF and FBI Integrated Automated Fingerprint Identification System (IAFIS) systems share data but the FBI will not have any direct access to the data within the AEF processing environment. The AEF application interfaces with the IAFIS FBI System using communication and data exchange protocols defined by the IAFIS system. This capability is implemented by AEF. An FBI dedicated Virtual Private Network (VPN) router connects the AEF system to the FBI IAFIS system over the Internet. The FBI VPN router encrypts/decrypts traffic between the IRS and FBI. The FBI configures and manages this router. AEF will communicate and share data with IAFIS through Simple Mail Transfer Protocol (SMTP) email messages. This includes the submission of transactions to IAFIS, and the receipt of response transactions from IAFIS via email. AEF will communicate with a remote file-based archive using TCP/IP sockets on a configurable port number. The archive will reside on a remote system that provides file storage of FBI Search transactions for an infinite amount of time. The AEF Transaction Management Server (TMS) will contain a client software package that communicates only with the archive server software. The purpose of this software is to insert, retrieve, and delete transactions from the archive when an AEF administrator reviews and/or deletes an archived transaction through the AEF Archive Manager Software.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
The processed demographic and fingerprinting data will be retained for at least 3 years, and will be maintained in accordance with Records Disposition Handbooks, IRM 1.15.59.1 through IRM 1.15.59.32. All data meeting end of retention period requirements will be eliminated, overwritten, degaussed, and/or destroyed in the most appropriate method depending on the type of storage media used based upon documented IRS policies and procedures.

14. Will this system use technology in a new way?
Yes. The IRS utilizes AEF to provide electronic copies of applicant fingerprints from FD–258 paper forms to the FBI to conduct criminal background investigations.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. The system provides information that enables the IRS (sanctioned by the Taxpayer Browsing Protection Act of 1997) to identify, locate, and monitor both firms and individuals for the purpose of auditing, and to prevent the misuse of IRS services.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
Yes. The system provides information that enables the IRS (sanctioned by the Taxpayer Browsing Protection Act of 1997) to identify, locate, and monitor both firms and individuals for the purpose of auditing and to prevent the misuse of IRS services. Role–based Access Controls (RBAC) based upon user profile information will be used to help prevent unauthorized monitoring of IRS entities. In addition, auditing controls and intrusion detection systems are used by the IRS as deterrents to avoid exploitation of sensitive information by unauthorized entities.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
Yes. The system provides information that enables the IRS (sanctioned by the Taxpayer Browsing Protection Act of 1997) to identify, locate, and monitor both firms and individuals for the purpose of auditing and to prevent the misuse of IRS services.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Applicants will be able to correct information immediately through contact with an IRS Customer Representative of AEF, or a resubmitted FD–258 fingerprint card. Applicants will have the right to appeal rejection for participation in the e-file program as a result of the FBI background investigation results. There is an edit function for the information contained in AEF. Results sent back from FBI cannot be corrected, however, once an individual's information is entered in the system it can be removed via deleting the record from the software. This is a function of AEF managers or leads, and can be completed by all AEF users except those acting as fingerprint card scanners. There are no anticipated effects on the due process rights of taxpayers and employees due to derivation of data. Under IRS terms of agreement, all authorized IRS personnel will be restricted from selling, trading, giving, bartering, misusing or further disclosing taxpayer information without that taxpayer's specific consent.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
No. AEF is not a web–based system.

View other PIAs on IRS.gov