Automated Electronic Fingerprinting (AEF) Phase II – Privacy Impact Assessment

PIA Approval Date – March 9, 2007

System Overview

Automated Electronic Fingerprinting (AEF) provides for sending scanned fingerprints to the Federal Bureau of Investigation (FBI) electronically. E-file providers must submit fingerprints as part of the criminal background evaluation. AEF coverts the manual, paper-based fingerprint process to an electronic means for transmitting to FBI's Integrated Automated Fingerprint Identification System (IAFIS).

Systems of Records Notices

- Treasury/IRS 22.062 - Electronic Filing Records.
- Treasury/IRS 36.003 - General Personnel and Payroll Records
- Treasury/IRS 34.021 - Personnel Security Investigation, National Background Investigation Center (NBIC)
- Treasury/IRS 34.027, IRS Audit Trail and Security Records System

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
- Social Security Number
- Place of Birth
- Date of Birth
- Date Fingerprinted
- Date Received
- 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
- Password

The SEID and Password are used by authorized IRS employees to logon to FCSS for authentication purposes.

C. Audit Trail
- Name

- SSN
- Barcode ID (each card has this ID attached 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 (Ex: complete, error, edit, search, etc…)

D. Other
The e-mail 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 e-mail can be either one of type types. Type 1: an e-mail notifying AEF that there was “no information found” on the individual. Type 2: an e-mail 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. Once FBI processing has been completed, FBI results will be transmitted, as an e-mail message, back to the AEF.

Phase II has enabled the automatic input of applicant demographic data into the TPDS whereupon TPDS triggers the transmission of TPDS selected FPCs and demographic information to the FBI via the AEF. FBI results are automatically input into TPDS from the AEF system.

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 and Applicant’s Name 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. The Federal Bureau of Investigation (FBI) provides the IRS with results of criminal background investigations through e-mail messages for use within the AEF system. This information automatically inputs into TPDS as part of an applicant's record. The data elements include FBI return actions of 'Data', 'No Data' or 'Unprocessible'.

D. There are no data elements obtained from State and Local Agencies for use within AEF other than those provided by the FBI.

E. There are no data elements obtained from third party sources for use within AEF other than those provided by the FBI.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All information used within the AEF processing environment is captured on the FD-258 fingerprint card and is necessary for the business purpose of the system.
The use of AEF technology including its interface with TPDS is both relevant and necessary for the purpose for which the AEF implementation was designed. This implementation has changed the current manual process of submitting fingerprint cards to the FBI for criminal background investigations. Response cycles are reduced from 30 days or more to 24 hours or less. Customer satisfaction and employee workloads are positively impacted.

4. How will each data item be verified for accuracy, timeliness, and completeness?
There is no additional data collected from any source other than the applicant's FD-258 fingerprint card. Currently, there is an automated 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.
The TPDS Component Interface (CI) with AEF automatically performs the following checks:

- **Validate SSN Check**: If SSN match with IRS records fails or no SSN is found, it will return a message back to Cogent stating *INVALIDSSN.* Cogent will inform the user by changing the ***Current State*** in the ***Site Transaction List*** to **INVALIDSSN** and the record will not be saved in TPDS.
- **Person Check**: Existence of individual in TPDS
  - If PERSON does not exists, a new person will be created in TPDS
  - If PERSON does exists, the First Name and Last Name will be updated if they are different from the IRS records
- **Suitability Check**: Existence of a Suitability record with the same date as the Requested Date
  - If a record exists, it will return a message back to Cogent stating *DUPLICATE.* Cogent will inform the user by changing the ***Current State*** in the ***Site Transaction List*** to **DUPLICATE** and the record will not be saved in TPDS.
- **FBI Check**: If the fingerprint card is chosen for background check or if the individual answered YES to one or more of the questions on the application concerning a criminal offense, it will return a message back to Cogent stating *SENDTOFBI.* Cogent will inform the user by changing the ***Current State*** in the ***Site Transaction List*** to **SENDTOFBI** and the record will be saved in TPDS. The 'Submit' button will then be activated on the ***Insert Demographics*** page allowing the user to send the card to the FBI via dedicated VPN tunnel.

In all other scenarios, it will return a message back to Cogent stating *COMPLETE.* Cogent will inform the user by changing the ***Current State*** in the ***Site Transaction List*** to **COMPLETE** and the record will be saved in TPDS.

5. Is there another source for the data? Explain how that source is or is not used.
No. There is 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 two ways. 1) An AEF user can query via Cogent GUI functionality using name or SSN, or barcode assigned to each fingerprint card. 2) An image of the actual fingerprint card is displayed and an AEF user (IRS employees only) can read the card for information.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. 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)?

Only IRS employees with appropriate roles and permissions have access to AEF. Contractors do not have access to AEF production systems. This PIA is applicable to FCSS components that operate within the production environment.

All AEF users, managers, system administrators and developers that have a need-to-know can access AEF data via Role-based Access Controls (RBAC).

The following chart details the roles and permissions of AEF users.

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

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

User Role: Archive Manager
IRS Role: Leads, Managers
Permissions: View previously archived transactions.

User Role: Lock Manager
IRS Role: Leads, Managers
Permissions: Unlock transactions that have been locked

User Role: Report Manager
IRS Role: Leads, Managers
Permissions: Generate and print identified reports

User Role: Barcode Printer
IRS Role: Leads, Managers
Permissions: Print barcode label

User Role: Database Administrator
IRS Role: Database Administrator
Permissions: Provides MS SQL Server Assistance/ Generate reports/ create ad hoc reports

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 IRS Online 5081 approval process.
Contractors do not have access to AEF components as part of the Production processing environment. Currently, any contractors acting as developers are required to have a Minimum Background Investigation (MBI)-level clearance to access the AEF developmental environment.

High-risk positions are subject to a full background investigation to include, for example, system administrators, shift supervisors or security operators. Full Background Investigations (BI) are normally performed for individuals with 'root' access to production systems per IRS standards.

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 applicant's SSN and full name via TIN Matching functionality by checking these data elements against TPDS. This check is not via manual comparison of the data and is done electronically.

In addition, TPDS stores calendar information within an applicant's profile of when he/she was fingerprinted and when his/her FPC was shipped to the FBI for a criminal history check. Once the FBI results are received by the IRS, the applicant's profile is updated to include the date that the results were received and the FBI response of *Data, No Data, **and/or Unprocessible.***

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)

- Previous PIA 3/3/2003, expired 3/3/2006
- C&A- 8/25/2005, expires 8/25/2008

Automated Electronic Fingerprinting (AEF)

- Phase I PIA, OPIP approved 11/15/2006

Privacy Impact Assessment for FBI Integrated Automated Fingerprint Identification System (IAFIS) is available at http://foia.fbi.gov/iafis.htm

12. Will other agencies provide, receive, or share data in any form with this system?
Yes. IRS AEF and FBI IAFIS systems share data but the FBI does 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 VPN router connects 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 communicates and shares data with IAFIS through Simple Mail Transfer Protocol (SMTP) e-mail messages. This includes the submission of transactions to IAFIS and the receipt of response transactions from IAFIS via e-mail. AEF communicates with a remote file-based archive using TCP/IP sockets on a configurable port number. The archive resides on a remote system that provides file storage of FBI Search transactions for an amount of time prescribed in IRM 1.15. The AEF Transaction Management Server (TMS) contains 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 2 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 is 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.

Background investigation results that are provided by the FBI contain criminal data on individuals. This information when received by authorized IRS employees may cause potential bias towards the individual depending on the criminal investigation results.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Applicants may correct information immediately through contact with an IRS Customer Representative of AEF or a resubmitted FD-258 fingerprint card. Applicants 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