Date of Approval: **August 4, 2015** PIA ID Number: **1435**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Automated Electronic Fingerprinting, AEF

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Automated Electronic Fingerprinting (AEF)

Next, enter the **date** of the most recent PIA. 10/2/2009

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above? No

If yes, explain what changes were made.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

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 and resides on MITS-30 GSS. Electronic Products and Services Support (EPSS) currently receives approximately 13,000 fingerprint cards a year, with the majority of submissions in August through December of each year. AEF is utilized to dramatically reduce the time and money required for the FBI to process the fingerprints for each individual. EPSS employees are the sole users of AEF. AEF uses the following process to scan a fingerprint card. An external e-file applicant is sent an official fingerprint card, which they must take to an approved office (such as a police station) to be fingerprinted. The card is then mailed to EPSS, who uses AEF to scan the cards and transmit a digital version of the fingerprints to the FBI (using a Secure Virtual Private Network (VPN) in Martinsburg). The FBI does a background check against the National Fingerprinting System and sends a secure e-mail with the results. The application consists of a Commercial Off-the-Shelf (COTS) application developed by Cogent Systems and several peripheral components. The application includes a Transaction Management Server, and a Database Server within the Enterprise Computing Center (ECC) - Martinsburg. Peripheral components include a Windows Common Operating Environment (COE) workstation, printer, scanner, and barcode reader located at the Andover, MA site. Fingerprint scanning and data entry only occur at the Andover, MA site. The Austin, TX site serves as the disaster recovery site for the production peripheral components. The system interfaces with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) system over the Internet. Cogent is designed to fully support fingerprint submission needs. The FCSS system provides the capability for scanning fingerprint cards (Cogent Document Scanner); storing fingerprint data in accordance (Cogent Archive Manager) with all applicable international standards; sending and receiving tenprint transactions (Cogent Transaction Manager); and sending/receiving messages containing the results of fingerprint searches performed by the IAFIS (Cogent Transaction Manager). The application transmits and retains copies of fingerprint cards which contain personal identifiable information, including name, date of birth, and Social Security Number, which is used by the FBI to perform criminal background checks for external e-file applicants. VPN is established by FBI and an MOU/ISA is in process of being signed. 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 system uses a dedicated SMTP Service and is connected to IAFIS FBI along the VPN routing path. AEF system utilizes Symantec's antivirus software to filter incoming and outgoing e-mail traffic. The Symantec Mail Security with AntiVirus V 5.0 software runs on a dedicated Wintel Server and is connected directly to the IRS NAT router

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes	On Primary	No	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

Yes	Social Security Number (SSN)

No	Employer Identification Number (EIN)
No	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Preparer Taxpayer Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or variations of SSN s).

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed by the FBI and is required by the FBI. There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system at the present time.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
No	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
Yes	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its

		mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

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 application transmits and retains copies of fingerprint cards which contain personal identifiable information, including name, date of birth, and Social Security Number, which is used by the FBI to perform criminal background checks for external e-file applicants.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

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 (Ex: complete, error, edit, search, etc.)

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
IRS 22.062	Electronic Filing Records
IRS 36.003	General Personnel and Payroll Records
IRS 34.021	Personnel Security Investigations, National Backgr
IRS 34.037	Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. N/A

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Federal Bureau of Investigations	FBI IAFIS system	Yes

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Form FD-258 (FBI Fingerprint Card)	FBI IAFIS system over the Internet	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
The individuals providing the IRS their SSN and fingerprints on the FD-258 fingerprint cards are required if they want to participate in the e-file program. Collection and use of the data is outlined in Publication 3112, IRS e-file Application and Participation. For the Acceptance Agent Application (AAA) program, applicants are told in the Form 13551, Application to Participate in the IRS Acceptance Agent Program instructions about the submission of the data and how it will be used.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
Applicants are submitting the necessary information voluntarily to participate in e-file and the AAA programs.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Applicants will be able to correct information immediately through contact with an IRS Assistor for either the e-file or the AAA programs. they may also opt to submit another FD-258 fingerprint card if they feel the fingerprints submitted were not of good quality. Additionally, applicants have the right

to appeal rejection from participation in the e-file and/or AAA programs as a result of the FB background investigation results.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level(Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	No	
Developers	No	

Contractor Employees? No

Contractor Employees?	Yes/No	Access Level	Background Invest.
Contractor Users			
Contractor Managers			
Contractor Sys. Admin.			
Contractor Developers			

21a. How is access to SBU/PII determined and by whom? Access is determined by business need through Management.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act? Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

The National Archives and Records Administration (NARA) approved the destruction of scanned AEF copies of fingerprint cards 3 years after the e-file provider has been dropped (Job No. N1-58-09-42, approved 9/2/09). This data retention requirement is published in Records Control Schedule (RCS) Document 12990 under RCS 29 for Submissions Processing Campus Records, Item 127. 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 10/2/2012

23.1 Describe in detail the system s audit trail. The AEF application is not documenting any critical elements in Appendix G. There are no files/tables that are updated and generated by the AEF application.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. N/A - AEF is in FISMA Non-Reportable Status.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: Under 100,000
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report