

Date of Approval: **August 15, 2019**

PIA ID Number: **4175**

## **SYSTEM DESCRIPTION**

*Enter the full name and acronym for the system, project, application and/or database.*

Automated Electronic Fingerprinting, AEF

*Is this a new system?*

No

*Is there a PCLIA for this system?*

Yes

*What is the full name, acronym and milestone of the most recent PCLIA?*

Automated Electronic Fingerprinting - AEF, 3475

*What is the approval date of the most recent PCLIA?*

7/2/2018

*Changes that occurred to require this update:*

New Interagency Use

*Were there other system changes not listed above?*

No

*What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.*

W&I Division Executive Resource Board

*Current ELC (Enterprise Life Cycle) Milestones:*

Operations & Maintenance (i.e. system is currently operational)

*Is this a Federal Information Security Management Act (FISMA) reportable system?*

No

## **General Business Purpose**

*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. The application consists of a Commercial Off-the-Shelf (COTS) application developed by Cogent Systems, and several other peripheral components. The application includes a Transaction Management Server, and a Database Server within the Enterprise Computing Center. Peripheral components include a Windows Common Operating Environment (COE) workstation, printer, scanner, and barcode reader. Designed to fully support fingerprint submission needs of AEF, Cogent, provides the capability of capturing scanned fingerprint cards and storing the fingerprint data in accordance with all applicable international standards. Cogent also provides the application the ability to send and receive transactions via Transaction Manager. To execute a transaction AEF interfaces with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) via the Internet, utilizing data exchange protocols and a dedicated two-way communication for data exchange. In parallel AEF interfaces with the FBI's Next Generation Identification (NGI) program (RAP BACK) via subscription maintaining integrity of suitability determinations over time.

## **PII DETAILS**

*Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?*

Yes

*Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?*

Yes

*What types of tax identification numbers (TIN) apply to this system?*

Social Security Number (SSN)

*List the approved Treasury uses of the SSN:*

Security Background Investigations

Interfaces with external entities that require the SSN

Delivery of governmental benefits, privileges, and services

Law enforcement and intelligence purposes

*Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)*

The SSN is a requirement and the significant part of the data being processed by the FBI which determines applicant suitability.

*Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).*

There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system at the present time.

*Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?*

Yes

*Specify the PII Elements:*

Name

Mailing address

Date of Birth

Place of Birth

Biometric Identifiers

*Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?*

Yes

*Specify the types of SBU from the SBU Types List (SBUList)*

Criminal Investigation Information - Information concerning IRS criminal investigations or the agents conducting the investigations.

*Are there other types of SBU/PII used in the system?*

No

*Cite the authority for collecting SBU/PII (including SSN if relevant)*

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

*Has the authority been verified with the system owner?*

Yes

## **BUSINESS NEEDS AND ACCURACY**

*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 tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.*

Automated Electronic Fingerprint (AEF) is used to scan and transfer fingerprint card images to the Federal Bureau of Investigation (FBI) for performing criminal background checks for e-file applications/applicants. AEF is utilized to dramatically reduce approval time for applicants and save resources used to make approval determination. The PII information is required for the FBI to process the fingerprints for individuals. Specifically, the application transmits and retains copies of fingerprint cards which contain personal identifiable information, including name, date of birth, and Social Security Number.

*How is the SBU/PII verified for accuracy, timeliness and completion?*

Information accuracy is based on FBI response to the fingerprints submitted by external customer. The AEF system is housed in a dedicated secured (locked) room. ALL SBU/PII data is scanned and housed in the secure area. AEF system software utilizes Barcode ID, each card has an ID attached to it so that any transaction that occurs is systemically notated with Barcode ID. AEF now interfaces with the FBI's RAP BACK program which provides alerts of event(s) that potentially impacts previous application determinations adding another layer of verified accuracy.

## **PRIVACY ACT AND SYSTEM OF RECORDS**

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

*Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.*

Yes

*Identify the Privacy Act SORN(s) that cover these records.*

IRS 22.062 Electronic Filing Records

IRS 36.003 General Personnel and Payroll Records

IRS 34.021 Personnel Security Investigations

IRS 34.037 Audit Trail and Security Records System

## **RESPONSIBLE PARTIES**

*Identify the individuals for the following system roles:*

## For Official Use Only

## **INCOMING PII INTERFACES**

*Does the system receive SBU/PII from other systems or agencies?*

Yes

*Does the system receive SBU/PII from IRS files and databases?*

No

*Does the system receive SBU/PII from other federal agency or agencies?*

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).*

Name: Federal Bureau of Investigations (FBI)

Transmission Method: VPN

ISA/MOU: Yes

*Does the system receive SBU/PII from State or local agency (-ies)?*

No

*Does the system receive SBU/PII from other sources?*

No

*Does the system receive SBU/PII from Taxpayer forms?*

Yes

*Please identify the form number and name:*

Form Number: Form 13551      Form Name: Application to Participate in the IRS  
Acceptance Agent Program

Form Number: Publication 3112      Form Name: IRS e-file Application and Participation

Form Number: FD-258      Form Name: Fingerprint Card

*Does the system receive SBU/PII from Employee forms (e.g. the I-9)?*

No

## **DISSEMINATION OF PII**

*Does this system disseminate SBU/PII?*

Yes

*Does this system disseminate SBU/PII to other IRS Systems?*

No

*Does this system disseminate SBU/PII to other Federal agencies?*

Yes

*Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).*

Organization Name: Federal Bureau of Investigations (FBI)

Transmission Method: VPN

ISA/MOU Yes

*Identify the authority*

MOU under the authority provided by Title 28, United States Code, Section 534 and 28 U.S.C. Section 534. The authority under which the IRS submits fingerprints for a criminal history background check is Treasury Department Circular No. 230.

*Identify the Routine Use in the applicable SORN (or Privacy Act exception)*

Collection and use of the data are outlined in Publication 3112, IRS e-file Application and Participation.

*For what purpose?*

Acceptance Agent Application (AAA) program

*Does this system disseminate SBU/PII to State and local agencies?*

No

*Does this system disseminate SBU/PII to IRS or Treasury contractors?*

No

*Does this system disseminate SBU/PII to other Sources?*

No

## **PRIVACY SENSITIVE TECHNOLOGY**

*Does this system use social media channels?*

No

*Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?*

Yes

*Briefly explain how the system uses the referenced technology.*

The system scans & transfers images of Fingerprints (biometrics) for comparison against FBI database for criminal background.

*Does the system use cloud computing?*

No

*Does this system/application interact with the public?*

No

## **INDIVIDUAL NOTICE AND CONSENT**

*Was/is notice provided to the individual prior to collection of information?*

Yes

*How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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 are 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.

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

Yes

*Describe the mechanism by which individuals indicate their consent choice(s):*

Applicants are voluntarily submitting the necessary information to participate in e-file and the AAA programs. Consequently, applicants can choose to not to participate.

*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 FBI background investigation results.

## **INFORMATION PROTECTION**

*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

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

*IRS Employees*

Users: Read Write

Managers: Read Write

*How is access to SBU/PII determined and by whom?*

Access is determined by business need through Management.

## **RECORDS SCHEDULE**

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?*

Yes

*How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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.

## **SA&A OR ASCA**

*Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?*

No

*Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?*

Yes

*Describe the system's audit trail.*

AEF system software utilizes Barcode ID (each card has this ID attached to it so that any transactions that occurs to the card will be notated. Beyond the Barcode ID 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. By contract (Memorandum of Understanding/Service Level Agreement) AEF must maintain the two-way dedicated communication. Any additional connections are to be negotiated.

## **PRIVACY TESTING**

*Does the system require a System Test Plan?*

No

*Please explain why:*

N/A - AEF is in FISMA Non-Reportable Status.

## **SBU DATA USE**

*Does this system use, or plan to use SBU Data in Testing?*

No

## **NUMBER AND CATEGORY OF PII RECORDS**

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

## **CIVIL LIBERTIES**

*Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?*

No

*Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?*

No

*Will this system have the capability to identify, locate, and monitor individuals or groups of people?*

No

*Does computer matching occur?*

No

## **ACCOUNTING OF DISCLOSURES**

*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