Date of Approval: **March 04, 2020**

PIA ID Number: **4556**

SYSTEM DESCRIPTION

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

Enterprise Electronic Fax, Release 2, EFS, EFS

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?

PCLIA # 1984 for 'Enterprise Electronic Fax, Release 2

What is the approval date of the most recent PCLIA?

1/24/2017

Changes that occurred to require this update:

Expiring PCLIA

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.

Information Technology Executive Steering Committee.

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?

Yes

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.

Enterprise Electronic Fax Release 2, also known as Enterprise Fax Storage (EFS) will receive electronic faxes delivered from the Enterprise Electronic Fax (EEFax) server and will be delivered and stored in a secure file repository located within the Enterprise Document Management Platform (EDMP) covered under PIA #3787. In order to increase employee efficiencies, curtail paper usage, and reduce overall operational costs, the IRS must address alternative methods of receiving, processing, and archiving electronic faxes. There are numerous operational and cost deficiencies in the current fax process. The goal of the Enterprise e-Fax Solution is to allow the IRS to increase its technology offerings and provide a mechanism to further reduce IRS reliance on paper records, standalone fax hardware, consumables, and warehouse space. This can be accomplished by providing an Enterprise Fax Storage (EFS) solution. Electronic faxes delivered from the Enterprise Electronic Fax (EEFax) system will interface directly with the EFS which will be established utilizing the Enterprise Document Management Platform (EDMP). This secure, scalable, and reliable enterprise document and record management environment will provide workflow capability and long-term archiving. Currently, electronic fax documents that are covered under retention rules incur significant costs resulting from being printed and physically stored at the Federal Records Center. The EFS system will allow users to quickly retrieve fax documents electronically, while reducing costs and improving efficiencies. Due process for records in the system is provided by statutes applicable to such records by processes external to the system.

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:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Delivery of governmental benefits, privileges, and services

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

The system is used to store IRS Tax Form 4506-T. Tax Form 4506-T is used to order a tax payer's transcript or other return information. The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. ISR-S requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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

EFS plans to mitigate the use of SSNs (or tax identification numbers) through a secure infrastructure that provides administrative and technical controls to secure PII data. Standard security features include user authentication for verification that the user is a valid repository user. User authentication occurs automatically, regardless of whether repository security is active. Password encryption protects passwords stored in a file. The Documentum Content Server automatically encrypts the passwords it uses to connect to third-party products, such as a Lightweight Directory Access Protocol (LDAP) directory server or the Relational Database Management System (RDBMS), and the passwords used by internal jobs to connect to repositories. User privileges define what special functions, if any, a user can perform in a repository. Folder security is an adjunct to repository security. Using encrypted file stores provides a way to ensure that content stored in a file store is not readable by users accessing it from the operating system. Auditing and tracing are optional features that you can use to monitor the activity in your repository. The EFS system uses EFTU in conjunction with Tectia to provide the required cryptographic protections for data in flight or in transition that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The General Support System (GSS)-24 and GSS-30 GSSs utilize encryption to protect PII data at rest. Back-Up Tapes: GSS-24 and GSS-30 GSSs uses the IRS Veritas Netbackup Solution for tape backup. Veritas encrypts all backup tapes utilizing FIPS 140-2 validated encryption. Application Servers: IRM 10.8.1.5.6 (12) states that encryption of data residing on the primary stored devices of IRS information systems (e.g., servers, mainframes) is not required. The GSS-24 and GSS-30 GSSs environment, in accordance with the IRM, has employed the following due diligence methods for protecting the EFS PII data that resides on the servers: (1) EFS enforces least

privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties. (2) EFS does not routinely print any documents. If required, printing is limited to the specific reason for printing any document. (3) EFS has had a Security Impact Analysis (SIA). (4) Physical security is an inherited control by EFS at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan.

Employer Identification Number

Other Taxpayer Identification Number

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

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Tax Account Information

Centralized Authorization File (CAF)

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

No

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.

The business need is based on allowing tax specialists to make determinations related to taxpayer income verification, filings, and liability. Once the document is archived, the PII will be used to allow for the successful electronic retrieval of these documents.

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

Users will validate the faxed information prior to entry. The EFS system identifies and enforces which fields are required to be completed before a record can be saved. Data validation checks are automated in the system to ensure date fields are valid dates and numeric fields are numeric. Automated business rules check to ensure information is complete and will cite what information might be missing. The technical specialist reviews the business rules findings and makes the final determination on completeness and can overrule the business rules if necessary.

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 36.003 General Personnel and Payroll Records

IRS 34.037 Audit Trail and Security Records

IRS 00.001 Correspondence Files and Correspondence Control Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

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?

Yes

Enter the files and databases:

System Name: Enterprise Electronic Fax (EEFax)
Current PCLIA: Yes
Approval Date: 3/21/2019
SA&A: Yes
ATO/IATO Date: 7/3/2018

System Name: General Support System (GSS)-30 (Active Directory)
Current PCLIA: Yes
Approval Date: 9/7/2018
SA&A: Yes
ATO/IATO Date: 6/3/2019

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

No

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 4506T Form Name: Request for Transcript of Tax Return

Form Number: Form 4506T-EZ Form Name: Short Form Request for Individual Tax Return Transcript

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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.?

No

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?

This is a taxpayer initiated action; they can decline to provide information by not sending the fax. Notice, consent and due process are provided in the tax forms and instructions filed by the taxpayer, and pursuant to 5 USC.

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):

This is a taxpayer initiated action; they can decline to provide information by not sending the fax. Notice, consent and due process are provided in the tax forms and instructions filed by the taxpayer, and pursuant to 5 USC.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

This is a taxpayer initiated action; they can decline to provide information by not sending the fax. Taxpayers are informed of their due process in the Electronic fax instructions. Notice, consent and due process are provided in the tax forms and instructions filed by the taxpayer, and pursuant to 5 USC.

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 Contractor Operated

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

IRS Employees

Users: Read Only

Managers: Read Write

System Administrators: Administrator

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Write

Contractor System Administrators: Read Write

Contractor Developers: Read Write

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

Users are authorized to use the system by their manager via the On-Line 5081 (OL5081) system. A potential user will request access via the OL5081 system. This request has to be approved by the potential user's manager based on a user's position and need-to-know. Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 process to request access to the System.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) 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.

Enterprise e-Fax is a service provider for the Business Unit. The electronic â€˜non-record' versions of the fax are purged systemically after a configurable retention period using the Biscom software's system configuration. The business unit will determine where the official recordkeeping copy of the document will reside for retention purposes. Records delivered to and housed in the Enterprise Document Management Platform (EDMP) system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. The Business Unit will follow mandatory disposition instructions under the IRS Records Control Schedules/General Records Schedules (RCS 8-37 published in Document 12990 and GRS 38-64 published in Document 12829, as appropriate) for the maintenance and destruction of all recordkeeping copies of faxed materials. Recordkeeping series identified as unscheduled and/or added to the EEFax Archive Site in future updates will be scheduled in coordination with the IRS Records and Information Management (RIM) Program Office.

SA&A OR ASCA

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

Yes

What date was it completed?

2/14/2019

Describe the system's audit trail.

Enterprise Fax Storage provides each fax with an audit trail. Auditing is performed at the server level and EFS maintains a log of all database activity. Data will be collected on employee audit trails include: Employee SEID; date and time of event; type of event; outcome status; source of event (workflow name/type); Metadata from the inbound fax (date, time, EEFax number, caller ID, response fax number, and number of pages).

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Continuous Monitoring (eCM) is performed annually to determine if selected System Security Plan (SSP) controls are operating as intended. The Security Assessment and Authorization (SA&A) process is conducted on a three year cycle whereby all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the SA&A are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings. EDMP is a secure infrastructure that provides administrative and technical controls to secure PII data. Standard security features include user authentication for verification that the user is a valid repository user. User authentication occurs automatically, regardless of whether repository security is active. Password encryption protects passwords stored in a file. The EFS Content Server automatically encrypts the passwords it uses to connect to third-party products, such as an LDAP directory server or the RDBMS, and the passwords used by internal jobs to connect to repositories. User privileges define what special functions, if any, a user can perform in a repository. Folder security is an adjunct to repository security. Using encrypted file stores provides a way to ensure that content stored in a file store is not readable by users accessing it from the operating system. Auditing and tracing are optional features that you can use to monitor the activity in your repository

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

The Security Assessment and Authorization (SA&A) process is conducted on a three year cycle whereby all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the SA&A are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

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: 50,000 to 100,000

Contractors: Under 5,000

Members of the Public: More than 1,000,000

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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

The audit trail includes employee's SEID, EEFax number, caller ID, and response fax number which can be used to identify an individual.

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