NOTE: The following reflects the information entered in the PIAMS Website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: 01/22/2014 PIA ID Number: **724**

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Enterprise Electronic Fax, EEFax

2a. Has the name of the system changed? Yes

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

Acronym changed from EEF to EEFax

3. Identify how many individuals the system contains information on

Number of Employees:	50,000 - 100,000
Number of Contractors:	Under 5,000
Members of the Public:	Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

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 processess external to the system.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 11/10/2010

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- **System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes)** Yes
- **System is undergoing Security Assessment and Authorization** No

6c. State any changes that have occurred to the system since the last PIA

EEFax receives facsimiles which come in the form of picture files which are converted to a Portable Document Format (PDF) file for delivery. The initial PIA stated 'the picture files will be stored only long enough for the system to verify delivery to the final destination'. This is still valid for the majority of electronic faxes; Release 2 now provides for electronic storage of some faxes within Documentum. These are faxes that would have been printed and stored in the

Federal Records Center in Release 1 of EEFax.

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	Yes	
		Other Source:
Other	No	

---

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

PII Name	On Public?	On Employee?
	No	No

10a. Briefly describe the PII available in the system referred to in question 10 above.

Enterprise Fax Storage collects and stores documents that are faxed in from taxpayers and others; the documents contain images (TIFF format) and are converted to PDF. The information may be written in a free-flow format or faxed copies of records, receipts and forms for documentation purposes. A SSN may potentially be included; the system only utilizes SSNs for the purpose of identifying and retrieving the documents.

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

The SSNs are only collected to allow the document to be indexed for future retrieval within Documentum.

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

The system receives faxed documents from taxpayer or preparers, if barcodes are used instead of SSNs the system will be able to read and route documents based on 2-D barcodes in accordance with the OMB memorandum M-07-16 which requires IRS to eliminate or reduce the unnecessary use of Social Security Numbers.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

The system receives faxes which may contain PII including Social Security Numbers. It is being configured to handle, route and store documents that are delivered to the system with 2-D barcodes once they are available and in production.

11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is <u>not</u> needed.

Enterprise Fax Storage provides each fax with an audit trail. Auditing is performed at the server level; Documentum (COTS software) maintains a log of all database activity. Data which 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, send fax number, number of pages).

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? <u>Yes</u>

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: <u>Yes</u>

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: <u>No</u>

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: <u>No</u>

If Yes, please list the agency (or agencies) below:

d. Third party sources: <u>No</u>

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): <u>Yes</u>

f. Employees (such as the I-9): <u>Yes</u>

g. Other: <u>No</u> **If Yes*, specify*:**

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

The business need is based on the type of fax received. In some cases it is to allow tax specialist to make determinations related to taxpayer filings and liability; in other instances, it will be used to conduct business of the government ie: hiring activities, invoice payment etc. Once the document is archived, the PII will be used to allow for the successful electronic retrieval of these documents.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration	Yes
To provide Taxpayer Services	Yes
To collect Demographic Data	No

For employee purposes	Yes	
		If other, what is the use?
Other:	Yes	To conduct business of the government ie: hiring activities, invoice payment etc.

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies		
Web Beacons		
Session Cookies		
Other:		*If other, specify:*

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Yes

18a. If Yes, how is their permission granted?

This is a taxpayer initiated action; they can decline to provide information by not sending the fax.

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent

Website Opt In or Out option

Published System of Records Notice in the Federal Register

Other:

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Contractor Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Only
Managers		Read Write
System Administrators		Read Write
Developers		No Access
Contractors:	Yes	
Contractor Users		Read Only
Contractor System Administrators		Read Write
Contractor Developers		Read Write
Other:	No	

If you answered yes to contractors, please answer 22a. *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level"background investigation? Yes

23. How is access to the PII determined and by whom?

Users are authorized to use the system by their manager via the On-Line 5081 (OL5081) system.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

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.

25. 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

25a. 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.

Enterprise e-Fax is a service provider for the Business Unit. The electronic '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 Documentum 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.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

Documentum 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 Documentum 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.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

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 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.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

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.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? No

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number	SORNS Name
• Treasury/IRS 36.003	General Personnel Records
• Treasury/IRS 34.037	-- IRS Audit Trail and Security Records System
• Treasury/IRS 00.001	Correspondence Files (including Stakeholder Relations)

Comments

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

32a. If Yes to any of the above, please describe:

NA

View other PIAs on IRS.gov