Date of Approval: January 24, 2017 PIA ID Number: **1984**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Enterprise Electronic Fax, Release 2, EFS

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.

Enterprise Electronic Fax, Release 2, EEF, 570, Approved

Next, enter the **date** of the most recent PIA. 2/5/2014

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

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**
Yes	**System Deployment/Milestone 5**
No	**Operations & Maintenance (i.e., system is currently operational)**

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

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.

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 but will be delivered and stored in a secure file repository located within the Enterprise Document Management Platform (EDMP) covered under PIA #961. 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.

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 tax identification numbers (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	**Social Security Number (SSN)**
Yes	**Employer Identification Number (EIN)**
Yes	**Individual Taxpayer Identification Number (ITIN)**
No	**Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)**
No	**Practitioner Tax Identification Number (PTIN)**

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 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. 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.

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	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	No
Yes	Place of Birth	No	No	No
Yes	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
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

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

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

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.

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
Treasury/IRS 36.003	**General Personnel Records**
Treasury/IRS 34.037	**IRS Audit Trail and Security Records System**
Treasury/IRS 00.001	**Correspondence Files**

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. Identify the individuals for the following system roles. ## Official Use Only

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? Yes

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
GSS-30 (Active Directory)	**Yes**	**01/26/2016**	**Yes**	**10/23/2013**

11b. Does the system receive SBU/PII from other federal agency or agencies? No

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

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

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

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

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

19. 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, and pursuant to 5 USC.

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 Contractor 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-Only**
Managers	**Yes**	**Read and Write**
Sys. Administrators	**Yes**	**Read and Write**
Developers	**No**	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	**Yes**	**Read-Only**	**Moderate**
Contractor Managers	**Yes**	**Read and Write**	**Moderate**
Contractor Sys. Admin.	**Yes**	**Read and Write**	**Moderate**
Contractor Developers	**Yes**	**Read and Write**	**Moderate**

21a. How is access to SBU/PII determined and by whom? 1. Users are authorized to use the system by their manager via the On-Line 5081 (OL5081) system. 2. 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. 3. 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.

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.

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 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.

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)? In-process

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 3/31/2017

23.1 Describe in detail the system s audit trail. Enterprise Fax Storage provides each fax with an audit trail. Auditing is performed at the server level; EFS 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).

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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?
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.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements 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

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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: 50,000 to 100,000
26b. Contractors: Under 5,000
26c. Members of the Public: More than 1,000,000
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