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: Apr 14 2014 12:00AM PIA ID Number: **825**

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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

Electronic Filing of 1041 Returns, EFS-1041

2a. Has the name of the system changed? No

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

3. Identify how many individuals the system contains information on

Number of Employees: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

Electronic Filing of 1041 Returns, hereafter referenced as EFS-1041, is an Internal Review Service (IRS) Wage and Investment (W & I) application that has been deployed since 1986. The application software is currently developed and maintained by Information Technology (IT) -- formerly MITS, Applications Development (AD) personnel located in New Carrollton, MD. The application is located and runs on UNISYS Mainframes (located in Enterprising Computing Center-Memphis (ECC-MEM) and Enterprise Computing Center-Martinsburg (ECC-MTB) under the purview of Modernization & Information Technology Services (MITS 23). The EFS-1041 application consists of a set of computer programs that process 1041 returns received electronically from preparers of business taxpayers. Correctly formatted information passes to the Generalized Mainline Framework (GMF) for ultimate posting to taxpayer accounts. The forms and records are posted in the Business Master File. Additionally, completed return data are output to the Tax Return Database (TRDB). Due process is provided pursuant to 26 USC.

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: 01/31/2012

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) No
- System is undergoing Security Assessment and Authorization Yes

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

None

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'. UII:015-000000223

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	No	
Other	Yes	*Other Source:* Federal Agency (PBGC); State Agency (ICON); Third Party (US Bank, State Qualified Plans, Vendors)

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)	No	No	No
Tax Payer ID Number (TIN)	No	No	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: No

PII Name	On Public?	On Employee?
	No	No

10a. What is the business purpose for collecting and using the SSN?

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.)

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

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

Describe the PII available in the system referred to in question 10 above.

Employer Identification Number (EIN), if any Business address Electronic File (e-File), Personal Identification Number (PIN), and Name Control (first four letters of the last name)

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 not needed.

EFS-1041 is maintained on a UNISYS mainframe and there are no users accessing the UNISYS mainframe. This is a batch file application.

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

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

a. IRS files and databases: Yes

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

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Electronic Management System (EMS)	Yes	07/11/2011	Yes	10/31/2011

b. Other federal agency or agencies: No

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

c. State and local agency or agencies: No

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

d. Third party sources: No

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

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No 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 data elements are required to carry out EFS-1041 business purposes, which are to validate 1041 returns and then process (e.g., extract and reformat) the tax return data for use with the other IRS systems.

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	No	
		If other, what is the use?
Other:	No	

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		
		If other, specify:
Other:		

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? No

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

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 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		No Access
Managers		No Access
System Administrators		Read Write
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
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?

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

EFS-1041 follows the On-Line 5081 (OL5081) process. Managers determine who is required to have access. Access is requested via the OL5081 system, approved by the employees' manager and granted by the system administrator.

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

1041 applies various methods to check for accuracy, timeliness and completeness. These methods include record counts as a verifier of accuracy and completeness. Validity checks are performed on the field lengths and types as the data are loaded. The Re-circulating Master file is checked to identify any data discrepancies. The Re-circulating Master File provides the history of the returns that are kept for the 1041 application by Employer Identification Number (EIN). There are file checkers that run at various points throughout the process to ensure that files have not been dropped. If the file counts do not balance, the 1041 process will stop.

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.

EFS data are approved for deletion/destruction when 1 year old, or when no longer needed for administrative, legal, audit or other operational purposes, whichever is sooner (Job No. N1-58-7-13, approved 2/9/98). These disposition instructions are published under IRM 1.15.32 Records Control Schedule (RCS) 32 for Electronic Tax Administration, Item 4 (soon to be re-published in Document 12990 as simply RCS 32). The authoritative datastore, however, for these electronically filed returns is the Tax Return Database (TRDB) with recordkeeping maintenance for six years in accordance with recently approved Job No. DAA-0058-2013-0004. TRDB disposition instructions will be published in Document 12990 under RCS 29, Item 445 when next updated.

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.

The 1041 application is internal to the IRS only. Employees are prohibited from extracting information and distributing from outside the IRS. Internal data transmissions are conducted using Electronic File Transfer Utility (EFTU), Network Data Mover (NDM), or File Transfer Protocol (FTP). While data exchanges between the 1041 system and the EMS system are sent via the insecure protocol, FTP.

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

For data at rest, 1041 follows all requirements in IRM 10.8.1.5.4.6(12), such as printing documents only necessary and required to support business processes and implementing security principles such as least privileges. 1041 follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest; users can only access information necessary to perform their job functions. The application adheres to the SA & A and physical security requirements set forth in IRM 10.4.1 – Physical Security Programs – Managers Security Handbook.

---

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 ConMon-R 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*? Yes

---

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

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

08/27/2012

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.

No SORN Records found.

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