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: October 9, 2014 PIA ID Number: **1056**

1. What type of system is this? Non-Major System

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

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

Financial Management Information System, FMIS

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

4. Responsible Parties:

NA

5. General Business Purpose of System

Financial Management Information System (FMIS) is an Internal Revenue Service (IRS) application/system that has been categorized as a Major Application. FMIS resides on the Modernized Information Technology Services (MITS)-21, IBM Master File General Support System (GSS), and is located at the Enterprise Computing Center in Martinsburg, WV (ECC-MTB). The FMIS Project is the primary source of reports and data used to prepare the IRS' Annual Custodial Financial Statements for the Government Accountability Office's (GAO) annual financial statement audits. IRS' Custodial financial statements are a significant part of Treasury's financial statements, which are compiled for the government-wide financial statements each year. Additionally, FMIS provides continuous and accurate responses to mandatory periodic and ad hoc requests for custodial financial reporting information from Treasury, Office of Management and Budget (OMB), Congress, and other government agency requests. FMIS has been operational since 1996, and directly contributes to the clean audit opinion on custodial financial statements the IRS has obtained from the GAO for the past ten consecutive fiscal years. FMIS contributes to accurate, transparent financial accounting on governmental operations to its citizens. The following sub-systems comprise the FMIS: Unpaid Assessments (UA), Revenue and Refunds (R&R), and Custodial Detail Database (CDDB). UA reports on the debit balance modules on the Individual Master File (IMF), Business Master File (BMF) and Non-Master File (NMF). Detail tax modules and entity records are created to summarize much of the data on the master files. This summarization includes defining the source of the assessment, the location of the module in the collection stream, the financial status of the module, and other profiling information. (The financial status is defined by determining if there is a two-party agreement on the amount due to the IRS.) This data is used in the financial statement audits by GAO, as a base for the Federal Payment Levy Program (FPLP) project, and for reporting debit balance modules both within and outside the agency. R&R is used to identify all the detail transactions that posted to IMF, BMF, and NMF during the fiscal year. At a high level, these detail transactions are broken down into Revenue transactions, Refund transactions, Other Transactions that are part of the fiscal year and Other Transactions that are not part of the fiscal year. Once these breakouts are done, revenue and refund reversal transactions are matched to the transactions they reverse. Paper and electronic reports are generated and distributed to Chief Financial Officer (CFO) Finance and GAO. The detail files provide support for the amounts reported from the Redesign Revenue Accounting Controls System (RRACS). The files are also made available to GAO for sampling and to validate the financial statements. The CDDB takes the lessons learned from prior modernization efforts to solve long-standing financial reporting weaknesses cited by GAO. The CDDB determines the amount of duplicate penalties assessed for financial reporting in the annual audit. It provides information on incorrect, missing, or invalid cross references to the business units for correction, improving the quality of the Trust Fund Recovery Penalty (TFRP) inventory. It provides transaction level support for the revenue and refund records in RRACS and improves the timeliness of financial information by providing data weekly instead of monthly. CDDB is the custodial sub-ledger that supports the financial statement and reconciles to the General Ledger

RRACS. FMIS does not directly interface or interconnect with any systems (internal or external). The application solely shares information with a number of different IRS internal systems via the IBM Mainframe (MITS-21 GSS).

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: 6/29/2011 12:00:00 AM

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

No changes.

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'. 015-45-01-01-01-2425-00

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

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 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

No Other PII Records found.

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

Each data item is necessary in support of the IRS custodial finance statement audit. FMIS supplies reports and data used to prepare the IRS custodial financial statements and supports the GAO Annual Fiscal Year Financial Statement Audit. IRS custodial financial statements are a significant part of the overall Treasury financial statements compiled for the government-wide financial statements each year and are audited by GAO.

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.)

26 USC 3402, 3406, 1441 and IRC 6109.

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

There is no alternative to the use of SSN.

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

There is no planned mitigation strategy and forecasted implantation date to mitigate or eliminate the use of SSNs in FMIS.

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

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.

FMIS does not have an audit trail.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

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

a. IRS files and databases: No

b. Other federal agency or agencies: Yes

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

GAO Lockbox

c. State and local agency or agencies: No

d. Third party sources: No

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.

Each data item is necessary in support of the IRS custodial finance statement audit. FMIS supplies reports and data used to prepare the IRS custodial financial statements and supports the GAO Annual Fiscal Year Financial Statement Audit. IRS custodial financial statements are a significant part of the overall Treasury financial statements compiled for the government-wide financial statements each year and are audited by GAO.

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	No	
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.) Yes

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)	Yes	GAO, Lockbox	Yes
State and local agency (-ies)	No		
Third party sources	No		
Other:	No		

** 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? Not Applicable

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

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	No
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	No
Other:	No

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		Read Only
Managers		Read Only
System Administrators		Read Write
Developers		Read Only
Contractors:	Yes	
Contractor Users		Read Only
Contractor System Administrators		Read Write
Contractor Developers		Read Only
Other:	No	Read Only

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?

Managers and Contracting Officer’s Technical Representatives (COTR) determine access. Access is granted to individuals on a “need to know” basis. On-Line 5081 (OL5081) has to be completed in order for access to be granted. Because this is a steady stack legacy system, programmers require access for continued maintenance. FMIS require programmers and report preparers to be authorized.

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

There is no direct user input to the FMIS system. All data is received from other systems. The forms themselves are input into the feeder systems (IDRS/Masterfile). FMIS receives the data from the MITS-21 GSS. To ensure no data is lost, the Log Accounting Report System (LARS) is used to ensure that the number of records sent matches the

number of records received by FMIS. Validity and accuracy of that data is the responsibility of the systems that provide data to FMIS.

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? No

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.

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.

A request for records disposition authority for FMIS and associated records will be drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for FMIS inputs, system data, outputs and system documentation will be published in Records Control Schedule (RCS) Document 12990 under RCS 16 for the Chief Financial Officer, Item 19. A 5-year retention has been proposed for Custodial Detail Database (CDDB) records. This mirrors approved disposition for similar budget reporting records approved under NARA's General Records Schedule. Once the retention period has expired, a batch purge program will identify all records that are more than 5 years old and remove them. The database shall be backed up prior to running the batch purge program. FMIS data queries of IMF, BMF and ANMF are stored in a flat file on the IBM mainframe. The proposed retention period for these files is 18 months, unless a customer specifically requests a longer retention period.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
FMIS resides on the MITS 21-GSS. There are no users with direct access to FMIS.

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

FMIS audit trail protection is provided by the MITS-21 GSS, System of Records Notice Number: Treasury/IRS 34.037.

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.

FMIS does not deal directly with taxpayers. Data is extracted on a weekly basis and loaded into other IRS systems which provide read only access to the data. The system provide the authorization, control and monitoring of access.

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)*? No

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.

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