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: 02/21/2014 PIA ID Number: **764**

1. What type of system is this? Modernized System

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

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

Modified Employee Plan / Exempt Organization Determination System, MEDS

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:	100,000 - 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The Modified Employee Plan / Exempt Organization Determination System (MEDS) provides full inventory and status control of determination cases and supports timely and accurate processing of applications for Employee Plans (EP) and Exempt Organizations (EO) determination letters as mandated by the Internal Revenue Code (IRC) and Income Tax Regulations.

The following is a description of the functions within MEDS:

- In the Receipt and Handling function users receive paper documents and image them in electronic form. All users are located within the Cincinnati Submission Processing Center (CSPC) facility and access the Captiva client application loaded on their workstations. This function is interconnected with the Business Rules function via the IRS/Treasury Intranet. This function interfaces with the IRS system CRX.

- In the Business Rules function the data from the cases is used to govern functionality associated with: Case Grading, Case Classification/Complexity, User Fee correctness, Case Categorization, Cycle, Application Completeness, Disclosability, and EP Case Closing and Notice Composition. The Business Rules function is interconnected with the Records Repository function and receives data from the Receipt and Handling function.

- In the Record Repository function case records are managed, assigned and processed by users. The Record Repository also supports the Business Rules and Reporting functions, and sends case status information to EDS.

- In the Reporting function the reporting capability support the Receipt and Handling and Record Repository functions along with EDS. The Receipt and Handling reporting capability is located in Covington, KY and includes all SQL Reporting services. The Record Repository reporting functionality however, is installed at ECC-MEM and utilizes Business Objects and the COTS product, Documentum. This is a repository for snapshots of case data from MEDS. It generates standard reports, queries, and ad-hoc reports from the case data and snapshots. Business Objects, and the COTS product, Documentum are both reporting capabilities the back-end utilizes. The Business Objects reporting functionality receives source data from the EDS legacy system. 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: 10/29/2010

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)** No
- **System is undergoing Security Assessment and Authorization** No

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

N/A

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'. 015-45-01-14-02-2480-00

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

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

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Phone Number	Yes	Yes
Plan Sponsor	Yes	No
Employer's Name	Yes	No
Contact Person's Name	Yes	No
Employee Group Number	No	Yes
Standard Employee Identifier	No	Yes

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

The MEDS application collects the following Taxpayer information:

Organization/Taxpayer Name, Taxpayer ID Number, Organization Address, Organization Phone Number, Plan Sponsor, Employer's Name and Contact Person's Name. MEDS also collects employee information, which includes the Employee Name, Employee's City and State, Employee Phone Number, Employee Group Number and Standard Employee Identifier (SEID).

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?

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.

MEDS maintains an application Audit Trail (also known as case chronology). Scanning auditing is conducted through use of Captiva (COTS software), this auditing of users is conducted at the GSS level after each of the

following actions:

- Scan
- Package review module checks contents of package (QA step)
- Image quality assessment (skew, de-skew)
- Pages are identified for OCR (based on form)
- Package submission
- OCR is performed These audit records are stored in a proprietary database using InputAccel, and may only be viewed by privileged managers with access to the Manager's Console. Following an audit triggered by Captiva, Documentum (COTS software) maintains a log of all database activity.

The MEDS application Audit Trail includes the following information:

- Successful Logons or logoffs
- Unsuccessful logons
- Change Of Password (use of identification and authentication mechanisms)
- Data files opens and closed (Introduction of designated objects into a user's address space)
- Specific Actions, such as reading, editing, deleting records or fields within Open and Closed Cases

- Creation, modification and deletion of designated objects
- Change in access control permissions
- User annotations made for each access or change made to the case
- Startup of a MEDS application component
- Running/Printing/Updating Reports
- Audit Log starting and stopping
- Audit Log Full
- Audit Log Purge
- All SA actions while logged on as a SA
- Batch file modifications to database
- Direct manipulation of records in the database and bypassing MEDS
- Date
- Time (to the nearest second)
- User SEID
- Data Component where event occurred
- Type of Event (User, File or other resource effected)
- Action Taken (IP Address, System name)
- Case Number
- Disabled Auditable Events
- System Administrator Actions
- Added User
- Subject Identity (SEID, Group, Phone Number)
- Outcome of Event (success/failure)
- Unique identifier for each transaction (User Name, SEID, Application Name)
- Status_Code (effected by update)
- CASE_NUMBER (MEDS Case Number)
- DATE_CHANGED
- DATE_ENTERED
- USR_CODE (single MEDS User ID from Captiva)
- COMMENTS

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:

No System Records found.

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): Yes

f. Employees (such as the I-9): Yes

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.

All information is essential. All data items are used by management to support case inventory control, inventory monitoring (i.e., by group and specialist), as well as reporting functions. The data in MEDS is necessary for TE/GE to determine if potential tax-exempt entities submitting applications to Exempt Organizations (EO) and Employee Plans (EP) meet the law requirements of the Internal Revenue Code. EDS maintains inventory for cases being resolved under the Employee Plans Determination Letter Program and the Exempt Organizations Determination Letter Program. No data is redundant or unnecessary.

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:	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)	No		
State and local agency (-ies)	Yes	Hawaii, California, New Hampshire, Attorney General; California, Georgia, Pennsylvania - State Tax Officials	Yes
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		
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? 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? Yes

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

If an applicant receives a "negative determination" as to the exemption/qualification, the applicant is notified of a proposed adverse determination and is given an opportunity to protest before any final action is taken. Additionally, the applicant has the right to appeal a determination through the Appeals Division, (or EO Technical or EP Examination for certain cases). Taxpayers are provided the Specialist's contact information to discuss negative determinations or to update incorrect case information.

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

Only individuals who have been identified in the application's database table are authorized to access MEDS information. These users are IRS employees performing data entry, Secretaries, Reviewer, Agents/Tax Law Specialists, and Managers. System Administrators and Database Administrators have access to all data, system files, and functions required to carry out their assigned tasks and responsibilities. Developers do not have access to any production data.

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

Accuracy: Captiva is used for scanning and imaging all correspondence. Optical Character Recognition (OCR) is used to convert the hard copy text into a soft copy. MEDS users then use Captiva FormWare to correct and validate the data. The technical specialist will review each application for sufficient data necessary to scan the document. Timeliness: Captiva FormWare is used to check paper submission and the date stamped on the submission. Completeness: 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? 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.

MEDS is unscheduled. A request for records disposition authority for MEDS and associated records is currently being 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 MEDS inputs, system data, outputs and system documentation will be published in IRS Document 12990 under Records Control Schedule (RCS) 24 for Tax Exempt and Government Entities (TEGE), item number to be determined.

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

The MEDS system utilizes the Enterprise File Transfer Utility (EFTU) to encrypt data transferred between the interconnected applications. Data at rest is protected using the Guardian Edge Removable Storage (GERS) encryption solution. Both are recognized IRS standards for protecting data.

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

The MEDS system utilizes the Enterprise File Transfer Utility (EFTU) to encrypt data transferred between the interconnected applications. Data at rest is protected using the Guardian Edge Removable Storage (GERS) encryption solution. Both are recognized IRS standards for protecting data.

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.

Annual Enterprise Continuous Monitoring (eCM) activities take place to evaluate a subset of security controls associated with the system.

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? 09/30/2013

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 50.222	Tax Exempt/Government Entities Case Management Rec
Treasury/IRS 34.037	IRS Audit Trail and Security Records System

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