

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: 07/11/2014 PIA ID Number: 991

---

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 Master File Transcripts Requests (ELEC MFTRA), EMFTRA

---

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

---

The Franchise Taxpayer Board (FTB) customer sends a request, via Secure Sockets Layer (SSL), to the Secure Data Transfer (SDT) server. The SDT server transfers the request, using Enterprise File Transfer Utility (EFTU), to the UNISYS 6800 Mainframe. The SDT server also transfers at this time the same request file to the cov001cpshr1 server for monthly congressional reporting. The UNISYS mainframe runs a program called LF767 (a batch reformatting program) to format the records for subsequent processing through the Transcript Research System, which creates the transcripts which are then transmitted by EFTU to IRS FTB workstation. The transcripts are redacted by the Disclosure Officer and sent via EFTU to the Secure Data Transfer (SDT) server for pick-up by FTB customer.

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: 02/19/2011

---

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

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'. none

---

## 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 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	No	No	No

Additional Types of PII: Yes

<u>PII Name</u>	<u>On Public?</u>	<u>On Employee?</u>
BUSINESS TAX RETURN	Yes	No

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

Business tax return Information Public Yes Employees NO

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.)

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)

Not Applicable

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

Not Applicable



---

**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	California Franchise Tax Board	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:	_____	<i>If other, specify:</i> _____

---

**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

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"?

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? 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:**

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

**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?**

The IRS uses the On-Line 5081 (OL5081) to support the management of ELEC MFTRA accounts. When a user submits an OL5081 to gain access to the application, the Disclosure Manager receives a copy of the request via e-mail and can approve or deny access.

---

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

The data items are verified for accuracy, timeliness, and completeness prior to ELEC MFTRA accessing the files on the IRS FTB workstation.

---

**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.**

EMFTRA data is approved for deletion when no longer needed for operational purposes (NARA Job No. N1-58-09-93). These disposition instructions, as well as those for EMFTRA inputs, outputs and system documentation are published in IRS Records Control Schedule (RCS) Document 12990 under RCS 19 for Enterprise Computing Center-Martinsburg (ECC-MCC), item 76.

**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.**

No records are stored

---

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

ELEC MFTRA inherits all of its technical security controls such as identification and authentication, access controls, auditing controls, and system communications controls from the MITS 32 GSS workstation domain policy settings.

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

ELEC MFTRA inherits all of its technical security controls such as identification and authentication, access controls, auditing controls, and system communications controls from the MITS 32 GSS workstation domain policy settings. These controls also apply to the data at rest, in flight, and in transition.

---

**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.**

The Audit Logs (event logs) are picked-up by CyberSecurity on a regular basis

---

**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**

Treas/IRS 24.030 IMF

Treas/IRS 24.046 BMF

Treas/IRS 34.037 Audit Trail and Security Records System

**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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

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

Not Applicable

[View other PIAs on IRS.gov](#)