Electronic Master File Transcripts Requests (ELEC MFTRA) – Privacy Impact Assessment

PIA Approval Date – Feb. 23, 2011

System Overview:

Electronic Master File Transcripts Requests (ELEC MFTRA) programs are automated research tools that were developed to mass order Master File Tax Account (MFTRA) data in a batch mode. The data received is delivered in its raw form or can be customized to meet the needs of its customer. The IRS California Franchise Tax Board is the main user of the system. The 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 to the Cov001cpshr1 server. The mainframe runs a program called LF767 (a batch reformatting program) resulting in a transcript. The transcript is transferred from the mainframe to IRS FTB using EFTU.

Systems of Records Notice (SORN):

- IRS 24.030--Customer Account Data Engine (CADE) Individual Master File (IMF)
- IRS 24.046--CADE Business Master File (BMF)

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer
   - Name
   - Tax return information
   - Account transcript
   - Tax period

B. Audit Trail Information – The ELEC MFTRA application does not perform any auditing and relies on the Windows XP workstation on which it resides to meet auditing requirements. The workstation is configured to capture audit events in accordance with IRM 10.8.3.

C. Other – 6103D Accounting for Disclosure – Requires supervisor's signature from person requesting the information and the signature of FTB Coordinator. Paper copies of the employee request for transcript data are retained at the Franchise Tax Board.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS FTB workstation shared directory provides:
   - Taxpayer (Individual or Business)
   - Name
   - Tax return information
   - Account transcript
   - Tax period

3. Is each data item required for the business purpose of the system? Explain.
No. Only the IRS data element is required. The business purpose is to redact sensitive information contained in the transcripts prior to the FTB customer receiving the transcripts.

4. How will each data item 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.

5. Is there another source for the data? Explain how that source is or is not used.
No. There are no other sources of data.

6. Generally, how will data be retrieved by the user?
Disclosure uses ELEC MFTRA to access data on the IRS FTB workstation via an active directory share for review and redacting the files.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
No, there is no search functionality. The user simply opens a flat file and has access to all of the data elements within the file.

<u>Access to the Data</u>

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

Role: Disclosure Employees
Permission: Disclosure Employees are responsible for reviewing and modifying the transcripts returned from the mainframe to ensure that sensitive information inappropriate to share with the state is removed from the transcript data file. Any item removed is replaced with a standard response letting the state know that a record was removed by the Disclosure office. These users have full access to the transcript file and are able to read, update and delete the file.

Role: Developers
Permission: The Developers are responsible for the development and support of the application functionality and modifies the application source code. Developers are responsible for the ongoing application maintenance and updates of the source code. The Developers do not have access to the ELEC MFTRA production environment. Developers do not function as end users within the application.

Role: System Administrators
Permission: Systems Administrators (SAs) are Modernization & Information Technology Services (MITS) – End User Equipment and Services (EUES) employees. SAs have full Operating System (OS) level administrative control over the Windows XP workstation and are also responsible for maintaining the ELEC MFTRA hardware and operating system and installing new versions of ELEC MFTRA. SAs do not function as end users within the application.

Role: Account Administrators
Permission: Account Administrators create and add user accounts to the domain after the user has been approved via OL5081. The Account Administrators is also responsible for

modifying user access, disabling and re–enabling user access, and terminating user accounts. Account Administrators do not function as end users within the application.

Note: Contractors do not have access to the data.

9. How is access to the data by a user 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.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
No, ELEC MFTRA does not provide, receive, or share data with other IRS systems.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Not Applicable.

12. Will other agencies provide, receive, or share data in any form with this system?
No, ELEC MFTRA does not provide, receive, or share data with other IRS systems. The Windows COE XP Workstation used by the Disclosure employee to access the transcripts is a standalone workstation and has no interconnections with any systems/application, internal or external to the IRS.

<u>Administrative Controls of Data</u>

13. What are the procedures for eliminating the data at the end of the retention period?
ELEC MFTRA data is approved for destruction when no longer needed for operational purposes in accordance with IRM/Records Control Schedule 19 for the Enterprise Computing Center – Martinsburg, Item 76 (Job No. N1–58–09–93). That National Archives–approved job number also provides (temporary) dispositions for ELEC MFTRA inputs, outputs and system documentation.

14. Will this system use technology in a new way?
No. ELEC MFTRA will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. The system will not be used to identify or locate individuals or user groups.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No. The application does not provide the capability to search to target, profile, or otherwise monitor the behaviour of individuals or groups fitting certain specified criteria.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. This application is solely used to retrieve previously processed taxpayer information; this information will not allow the IRS to treat anyone differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not applicable. ELEC MFTRA does not make determinations.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
ELEC MFTRA is not web–based.

View other PIAs on IRS.gov