Electronic Management System (EMS) – Privacy Impact Assessment

PIA Approval Date: November 19, 2010

System Overview:

The Electronic Management System (EMS) is a Critical Infrastructure Project located at the front end of the IRS electronic filing (e-File) systems. It receives Federal and state tax return files from Trading Partners via external transmitters. After validating transmission information, EMS makes the Federal returns (Forms 94x, 1040, 1041 and some stand alone tax documents) available for processing by IRS back end e-file processing systems. It makes the state returns (forms 1040 and 1041) available for participating states to retrieve and process, and allows the states to send EMS acknowledgment files for the originating transmitter of the state return to retrieve.

Systems of Records Notice (SORN):

- Treasury/IRS 22.062 – Electronic Filing Records
- Treasury/IRS 24.030 – CADE Individual Master File (IMF)
- Treasury/IRS 24.046 – CADE Business Master File (BMF)
- Treasury/IRS 34.020 – Audit Trail Lead Analysis System (ATLAS)
- Treasury/IRS 34.037 – IRS Audit Trail and Security Records System

Data in the System

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

EMS is a store and forward Front End Processor for IRS electronic filing of forms 94x, 1040, 1041, some stand alone tax forms, and state returns for 1040 and 1041. While taxpayer, employee, and trading partner data is in the system, no personally identifiable information (PII) is indexed or searchable in EMS. The following data passes through EMS.

A. Taxpayer: The Taxpayer in this instance is an individual or business entity subject to taxation or reporting under the United States Internal Revenue Code and filing or reporting electronically on the following families of forms: 940x; 1040; 1041; and some stand alone tax forms such as form 4868. These forms contain the following types of information:

- Legal names (As distinguished from doing-business-as name), including spouse and dependents names
- Doing-business-as name (if any)
- Address (number, street, P.O. Box)
- City, State, ZIP Code
- State Code for the state in which deposits were made ONLY if different from the identified address.
- Date quarter ended (941)
- Employer Identification Number (EIN) or Social Security Number (SSN) (self, spouse, dependents). Note: The EIN is not a PII data element.
- Adjusted Gross Income (AGI), taxable income, owed or refundable amounts
- Bank account information
- Deposit account information
- Date of Birth
- Personal Identification Number (PIN) signature

IRS requires taxpayers who electronically file 94x returns through a third party transmitter to register for a PIN that the filer or authorized person must use to sign the return. The EMS Customer Database issues the PIN after EMS receives and stores the following registration information:

- The name, address, and Employer Identification Number (EIN) of the filer submitting the application
- The name, title, and telephone number of the person to contact regarding the application
- The name of the person who is authorized to use the PIN
- The email address of the contact person

B. Employee:

- EMS System Administrators (SA) updates EMS with names of Help Desk Assistors, Systems Administrators, and Developer/Contractors to allow them access to EMS.
- EMS SAs can also update the EMS database with a suspension indicator, test/production indicator, and IP address.

C. Audit Trail Information: The EMS audit trail log is able to create and maintain an audit trail of user/system security-relevant events and protect it from unauthorized modification, access and destruction. The audit log contains only the user ID. There is no other employee information captured by these logs. For the Trading Partner (TP), only the Electronic Transmitter Identification Number (ETIN) is captured. There is no other information available to individually identify any user.

D. Other: Transmitters: EMS database(s) includes the following transmitter information:

- Company Name
- ETIN Note: the ETIN is not a PII data element
- User ID
- Password
- IP Address of File Transfer Protocol (FTP) transmitters
- Shared Secrets (Used for account management)

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

A. IRS: EMS obtains (uploads) from an IRS relay server a data extract that the IRS Third Party Data Store (TPDS) provides. The extract may contain the following data about the transmitters (including states):

- ETIN
- Name
- EMS Login ID,
- first time user password

B. Taxpayer: None.

C. Employee: An EMS System Administrator (SA) obtains from an employee requiring access to the EMS, an Online form 5081 (OL5081) Automated Information System User Registration/Change Request that contains the employee name for the SA to enter in EMS.

D. Other Federal Agencies: None.

E. State and Local Agencies: From states, EMS receives Acknowledgement (ACK) files that contain transmitters' ETINs as well as embedded SSNs. EMS does not index or retrieve any data in the ACK files except the ETIN. All other data in the ACK files including the SSNs just

pass through EMS. EMS validates the ETINs, which are not PII, and puts the ACK files in transmitters' outbound electronic mailboxes for the transmitters to pick up.

F. Other third party sources:
Transmitters: EMS receives data elements in files from e-file Transmitters:

- All transmission files contain all transmitter information data elements (see response to question 1 above). EMS only searches for and validates the ETIN.
- From transmission files containing PIN Registration requests, EMS receives employer firm information that includes the employer firm name, address, EIN, and a contact name.
- e-Help Assistors use the EMS Help Desk web interface to update the Customer Off-line Profile on the EMS system with the Employer firm information. They can search the record by EIN and request reports on recently received requests for PINs.
- To log into the EMS system, a trading partner provides EMS their User ID and password. EMS validates the ID and password against the EMS database profile. The password is encrypted.

3. Is each data item required for the business purpose of the system? Explain.
Yes. The data collected by the system is required for the business purposes of EMS.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The return data comes in from Trading Partner transmission files. EMS opens the files only to check accuracy of electronic format of the transmission file and forwards to the appropriate back end systems for processing. Any check for internal accuracy of return data occurs there, not in EMS. The "check" EMS performs is only on the electronic envelope (header and trailer) of each file transmitted. EMS authenticates the transmitter based on the User ID and password against their profile and validates the file format. The taxpayer data inside the file is not inspected until the file reaches the back-end system.

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?
IRS Help Desk personnel can access the transmission status data as they assist trading partners having difficulty submitting files because of file transmission problems. Help Desk personnel can view status of the file and provide feedback or correction for successful transmission.

In the rare event a Transmitter disputes an Error Reject from IRS, they can provide an EMS e-Help Assistor with a taxpayer's SSN that they believe should be in the file. The e-Help Assistor can use the SSN to search the file to see whether the return was transmitted as claimed.

- System Administrators – SAs can retrieve data through either their web-based access or administrator accounts depending on the specific requirement.
- Database Administrators, if required, would retrieve data through their administrator account.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. In the rare event a Transmitter disputes an Error Reject from IRS, they can provide an EMS e-Help Assistor with a taxpayer's SSN that they believe should be in the file. The e-Help Assistor can use the SSN to search the file to see whether the return was transmitted as claimed.

Access to the Data

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

- **Roles:** E-Help Assistors (Tax Examiners)
- **Permissions:** Help Desk personnel can enter search criteria and perform specific functions by selecting from drop down menus on the web interface. Certain roles within the Help Desk allow dates and GTX keys (unique date and time stamp of group of returns) to be modified. Basic Trading Partner account information can be viewed as well.

- **Roles:** Trading Partners (TELNET)
- **Permissions:** Trading partner's access permissions are limited to dropping off or picking up files in their drop box.

- **Roles:** Trading Partners (FTP)
- **Permissions:** Trading partner's access permissions are limited to dropping off or picking up files in their drop box.

- **Roles:** System Administrators and, DBAs
- **Permissions:** System and database administrators access the underlying operating system and RDBMS in performing administrative actions. Database administrators are not authorized to enter information directly into EMS. System Administrators can access EMS through their web-based access and do so depending on the action they must perform in the application.

- **Roles:** Contractors
- **Permissions:** The contract development is limited to read only access controlled through Firewall procedures.

9. How is access to the data by a user determined and by whom?
Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user be added. They must fill out OL5081, Information System User Registration/Change Request, to request access to the application. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on OL5081.

There are contractors acting as users of the system. Contractor users are required to complete the OL5081 process prior to receiving access to EMS. Additionally, access on the system is on a need-to-know basis and is restricted based on Operating System (OS) and application level permissions and Role-based Access Controls (RBAC). Trader Partner access to the drop boxes is controlled by TPDS. TPDS is outside of the scope of this PIA.

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.
EMS automatically forwards files, daily, to:

- Electronic Filing System (ELF) (Individual Returns) (ELF). ELF retrieves 1040 family returns and Electronic Tax Documents (ETDs) from EMS and validates and processes each return in a transmission before either rejecting it or accepting it and sending it further through the Generalized Mainline Framework (GMF), which merges electronic with paper returns prior to processing for Individual Master File posting.

- Electronic Filing System (EFS) (Business Returns) EFS. EFS returns are transmitted to EMS and sent to UNISYS for processing.

- 94X-XML. This system receives and processes Employment/Unemployment Tax (Form 94x) Returns and associated Electronic Payment Records from EMS in XML.

- Third Party Data Store (TPDS). This system is used to record and monitor the information about electronic return originators, transmitters, software developers, and Intermediate Service Providers who have applied to participate in e-file. TPDS sends data to EMS which includes the ETIN, username, password, and permissions for the types of forms the transmitter can send. The third party gets an ETIN in one letter and a separate letter with EMS login ID and one-time use password. TPDS is part of e-Services.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

ELF
- Security Assessment and Authorization (SA&A) Authority to Operate (ATO): 5/26/2009
- PIA: 4/15/2009

EFS
- ATO: 5/26/2009
- PIA: 1/5/2010

94X-XML
- ATO: 5/6/2010
- PIA: 2/26/2010

TPDS (part of e-Services) –
- ATO: 4/2/2008
- PIA: 1/26/2007

12. Will other agencies provide, receive, or share data in any form with this system?
No. No other agencies provide, receive, or share data in any form with EMS.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
EMS master data files are approved for destruction when 7 years old (Job No. N1-58-97-13), as published under IRM 1.15.35, item 8 Records Control Schedule for Tax Administration Systems (Electronic). Data files are retained near line for 14 days, and then removed to the back-end system for the duration of their required retention.

The Customer database used to produce the PINs is maintained for the filing season and then purged. No further scheduling action is required by the Records Office regarding the creation/destruction of PINs.

14. Will this system use technology in a new way?
No, they system 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. EMS has no functionality for the purpose of locating or identifying individuals or 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.
Yes. The system has the capability to monitor authorized internal and external users through the use of Identification and Authentication (I&A) techniques (i.e., User ID and password), in addition to the analysis of system security audit logs to detect unauthorized access/use, fraud, or abuse of IRS systems. All internal and external users received warning banners.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. EMS is a front end processor. It has no capability other than receiving, authenticating, temporarily storing, and forwarding data.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
No. No legal determinations are made on data passing through EMS. EMS does not regularly open the files it handles except to verify the format. In exceptional circumstances, EMS System Administrators may open an improperly identified file to determine its origin prior to destroying or re-routing it. The EMS SA may notify appropriate IRS personnel and/or transmitters that EMS did not process a file because it was not able to process it, or unidentifiable or that it contained viruses or XML vulnerabilities.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
No. The system does not use any persistent cookies or other tracking devices.

View other PIAs on IRS.gov