Electronic Management System (EMS) Processing Year 2008 – Privacy Impact Assessment

PIA Approval Date – Jan. 24, 2008

System Overview

The Electronic Management System (EMS) is an Infrastructure Project located at the front end of the IRS 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. EMS provides acknowledgements to its Trading Partners for files transmitted. EMS operates in a secure environment. All transmissions to and from the EMS are encrypted.

Systems of Records Notice (SORN):

- 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) update 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. . There is no other employee information captured by these logs. For the Trading Partner, only the 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
- Company Address
- Telephone Number
- Electronic Transmitter Identification Number (ETIN). Note: the ETIN is not a PII data element
- User ID
- Password
- IP Address of File Transfer Protocol (FTP) transmitters

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

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
- Address
- telephone number
- EMS Login ID,
- first time user password

Employee:
An EMS System Administrator (SA) obtains from an employee requiring access to the EMS, an SF5081 “Automated Information System User Registration/Change Request” that contains the employee name for the SA to enter in EMS.

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.

Other third party sources:

Transmitters: EMS receives data elements in files from e-file Transmitters:

- All transmission files contain transmitter information data elements (see 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 EMSEMS authenticates the transmitter and validates the file format.

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.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

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.

<u>Access to the Data</u>

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

- **Role:** IRS ALL Help Desk personnel
  Privileges: Access to transmission status data as they assist trading partners having difficulty submitting files because of file transmission problems

- **Role:** Personnel are IRS employees
  Privileges: May view some formatted EMS data and provide feedback or correction for successful transmission

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 Form 5081, 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 Form 5081.

There are contractors acting as users of the system. Contractor users are required to complete the 5081 process prior to receiving access to EMS. Additionally, access on the system is on a need-to-know basis and is restricted based on OS and application level permissions and Role-based Access Controls (RBAC).

Please note: "High risk" background investigations have been completed for contractors with sys admin privilege.

10. Do other IRS systems provide, receive, or share data in the system?
EMS automatically forwards files, daily, to:

- ELF programs receive 1040, stand alone tax documents, and state returns
- EFS programs receive 1041 and state returns
- 94x programs on a back end platform receive 94x returns

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

- ELF – ATO 6/7/2006, PIA information not available
- EFS – ATO 6/7/2006, PIA information not available
- 94x – ATO 6/8/07, PIA signed 7/24/2006

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

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Data files are retained for 14 days and then are removed to the back-end system.
The Customer database used to produce the PINs is maintained for the filing season and then purged.

14. Will this system use technology in a new way?
No

15. Will this system be used to identify or locate individuals or groups?
No. EMS has no defined 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? Explain.
No. EMS is a front end processor. It has no other capability 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. Legal determinations negative or otherwise 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 unprocessable 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?

EMS is not a Web-based system. Web interface is accomplished through devices that are managed by IRS Enterprise Networks. The Web interface is closed before any data is sent to the EMS. The e-Help assistors have a Web-based interface via the IRS Intranet only to look at the transmission status of files.

View other PIAs on IRS.gov