Employment Validation (EVA) – Privacy Impact Assessment

PIA Approval Date – May 7, 2007

Requested Operational Date – Currently Operational

Purpose of the System:

EVA is an up-front earnings validation and fraud detection program. EVA provides the ability to review employer or employee information on data received from state employment security commission files for a given Social Security Number (SSN) or Federal Employer Identification Number (FEIN). It displays which employers reported the taxpayer as an employee and if multiple individuals have used an SSN for their wage documents. It also provides employer contact information, if the IRS needs to contact the employer regarding the employee.

IRS receives this information under the authority of Memorandums of Understandings (MOUs) established between the Office of Disclosure and the States of California and South Dakota. The MOUs currently in place between IRS and California and South Dakota are as follows:

- Memorandum of Understanding between the Internal Revenue Service and the South Dakota Department of Labor Division of Unemployment Insurance effective Feb. 6, 1996.
- Memorandum of Implementation for the Agreement on Coordination of Tax Administration between the California Franchise Tax Board and the Internal Revenue Service effective Oct. 2, 2003.

The information contained within the MOU's will be examined within the next year to validate accuracy of the description of data used by Criminal Investigation.

EVA receives the data files quarterly from the California and South Dakota state agencies, as each quarter employers pay into the unemployment fund and must furnish the state with information about the amount of wages paid to employees. The state agency maintains accurate records of wages in order to determine the proper amount for unemployment checks, should the employee be laid off. The Federal Employer Identification Number (FEIN) is part of the EVA record as well as the state number. EVA is for IRS-internal use only, and is used by Criminal Investigation (CI) and Small Business-Self Employed (SBSE).

Systems of Records Notice (SORN):

- Treasury/IRS 46.009 – Centralized Evaluation and Processing of Information Items (CEPIIs)
- Treasury/IRS 34.037 – 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:

The Employment Validation system contains information on individuals that is supplied by the California Employment Development Department Tax Disclosure Office and the South Dakota Data Center Product Control. Information in the system includes:

A. Taxpayer:

- Employee Social Security Number (SSN)
- Employee name
- Employee address
- Employer name
- Employer address
- Federal Employer Identification Number (FEIN)

- Wages
- Account number

B. Employee: None.

C. Audit Trial Information:

- User ID of IRS employee
- Date time stamp
- Subject of the Event (SSN or FEIN)

D. Other: None.

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

A. IRS: None.

B .Taxpayer: Taxpayer and employer/payer information is submitted to the IRS quarterly via tapes from the California and South Dakota state agencies. The data is not directly collected from the taxpayer by EVA.

C. Employee Audit Trail Information:

- User ID
- Password

D. Other Federal Agencies: None

E. State and Local Agencies: The Employment Validation data files contain information on individuals that is supplied by the California Employment Development Department Tax Disclosure Office and the South Dakota Data Center Product Control. The state wage and employment tapes are sent on a quarterly basis to the Detroit Computer Service Center for processing.

Data elements obtained from California's Employment Development Department Tax Disclosure Office files:

- Employee SSN
- Employee name
- Employee address
- Employer name
- Employer address
- FEIN
- Wages
- Account number

Data elements obtained from South Dakota Data Center Product Control files:

- Employee SSN
- Employee name
- Employee address
- Employer name
- Employer address
- FEIN

F. Other third party sources: None

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data items compiled by the EVA are used as a screening tool and compared with W-2 data as filed on the taxpayer's return to validate wage and employment information that relates to potentially fraudulent tax returns. A determination is then made as to whether or not to pursue further verification of the W-2 data.

4. How will each data item be verified for accuracy, timeliness and completeness?
All data provided by the California and South Dakota state agencies is considered to be accurate and complete. Upon receiving the tapes, the programmer performs several checks to ensure the completeness of the data including:

- Ensuring that the number of tapes sent is the number received
- Verifying the correct block size
- Checking the data set name
- Ensuring that the file sent is the name of the file received.

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

6. Generally, how will data be retrieved by the user?
Once allowed access to the EVA main menu, the user retrieves the data by requesting information relating to a specific Taxpayer SSN or Employer FEIN via one of the menu options. The data can be retrieved as follows:

- Employment Processing – Search for employee wage information using a specific SSN
- Employer Information – Search for employer information using a specific FEIN
- Duplicate Name Search – Search for employee records under a specific SSN

Once the user has queried data using one of the methods above, the user has read-only access.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, data is retrievable by SSN or FEIN. Data must be queried by SSN because this is the format in which it is received from the state agencies.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
There are currently approximately 76 users (75 users from CI and 1 user from SB/SE). There are currently no contractors working on the system. The following categories of personnel will have access to data in the system:

- CI Investigative Analysts/Aides at the Fraud Detection Centers;
- System administrators at the Detroit Computing Center production site, and developers at the development site for troubleshooting problems within the application.

The users of EVA possess the following permissions:

- **Role**
  CI Investigative Analysts/Aides
  Permissions
  Query & read-only access.

- **Role**
  System Administrators

Permissions
Read/write rights to all levels of the EVA production environment, read access to the audit file, create user accounts, load data.

- **Role**
  Developers
  Permissions
  Maintains the application at the development site, obtains permission for production read-only for trouble shooting.

9. How is access to the data by a user determined and by whom?
Unique Resources Access Control Facility (RACF) user identifications are required for authentication to the mainframe. An OL5081 is required of IRS users requesting access to the mainframe and to EVA and must be signed by an immediate manager. All users have read-only access. Once forms are approved they are submitted to the System Administrator, who adds the new user's account into the system. The OL5081 process ensures that the user identifier is issued to the intended party and that user identifiers are archived.

User accounts are reviewed annually to ensure their access is appropriate as specified by their respective OL5081s and a user's access to the data terminates when it is no longer required or the employee leaves. This is controlled by the OL5081 process.

All users who access EVA are IRS employees, and access the application through an IRS workstation or laptop. Users access EVA through a terminal emulator, which must be installed on their desktop. Users must enter their unique RACF user identification and password before the terminal emulator will connect to the mainframe and the chosen application. Enterprise Remote Access Project (ERAP) controls are in place for remote 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. If NO, continue to Question 12.
No. EVA is not interconnected, nor shares information with any other system.

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?
The data contained in EVA are provided by California and South Dakota state employment agencies. These tapes are provided on a quarterly basis to the IRS. After they are successfully manually uploaded into the system the tapes are returned to the state agencies.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Records control is covered by IRM 1.15.30, Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003. The data in the system is updated quarterly as new tapes are received from the state agencies. Previous data in the system is overwritten.

EVA also follows disk sanitization procedures for destruction of discarded media as outlined in IRM 2.7.4, Management of Magnetic Media (Purging of SBU Data and Destruction of Computer Media).

14. Will this system use technology in a new way? If "YES" describe. If "NO" go to Question 15.
No.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. There is sufficient information in the system to locate and contact the employer to verify information. Once fraud is suspected, laws and administrative procedures, policies and controls govern the ensuing actions.

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.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.
No. Once fraud is suspected, laws and administrative procedures, policies and controls govern the ensuing actions.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
N/A - EVA is a research tool that assists the government in identifying possible criminal intent by a filer or a return preparer in submitting a fraudulent tax return. The system itself does not have the capability to assign any type of determination; however, CI awards due process during the subsequent investigation.

19. If the system is Web-based, does it use persistent cookies or other tracking devices to identify Web visitors?
N/A – EVA is not a Web-based system.

View other PIAs on IRS.gov