Employee Protection System (EPS) – Privacy Impact Assessment

PIA Approval Date – Mar. 20, 2009

System Overview

The purpose of Employee Protection System (EPS) is to catalogue information and data about Potentially Dangerous Taxpayer (PDT) and Caution Upon Contact (CAU) taxpayer cases. These cases identify taxpayers who represent a potential danger to the Internal Revenue Service (IRS) and/or IRS Employees including information that relates to the reasons why the taxpayer is considered a potential danger.

Systems of Records Notice (SORN):

- IRS 60.000–Employee Protection System
- 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:

A. Taxpayer – The EPS database contains information to identify taxpayers that represent a potential danger to the agency/employee including information that relates to the reasons why the taxpayer is considered a potential danger (description of incident). The data elements include:
   - Name
   - Social Security Number (SSN)
   - Employee Identification Number (EIN)
   - Address
   - Gender
   - Date of Birth (DOB)

B. Employee – The EPS database contains information to identify the employee who reported the incident. The data elements include:
   - Name
   - Phone number
   - Area Director's name
   - Area Director's phone number
   - Operating Division
   - Operating Unit
   - Position
   - Manager's name
   - Manager's phone number

C. Audit Trail Information– The Database Administrator is responsible for reviewing the audit trail logs, which identifies database activity by user identification.

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

A. Employee –The CAU data elements are:
   - Employee name

- Employee position
- Employee telephone number
- Employee office address
- Manager name
- Manager phone number
- Manager operating division and unit
- Manager area and group
- Taxpayer name
- Taxpayer SSN
- Taxpayer EIN
- Taxpayer home address
- Taxpayer gender
- Taxpayer DOB
- Brief description of incident

B. Other Federal Agencies: EPS data elements are received daily from TIGTA via SFTP scripts. The file that is sent by TIGTA contains information about the referral including:
   - Name
   - SSN
   - Address
   - Referring employee's name

   The data received is extracted from electronic Form 8273, Assault, Threat, and Harassment Incident Report. The Employee Protection Specialist located in the OEP inserts date and status information into the database. In order to conduct a thorough investigation, TIGTA gathers information from other Agencies such as the Federal Bureau of Investigation (FBI) and the National Crime Information Center (NCIC).

C. State and Local Agencies: Various state government agencies can provide data to EPS if the state agency has a Memorandum of Understanding (MOU) in place with the IRS Disclosure Office. The state agency government liaison sends data via postal mail or fax to the IRS Disclosure Officer for forwarding to the OEP. These data elements include:
   - Taxpayer name
   - Taxpayer SSN
   - Taxpayer address
   - Brief description of incident

3. Is each data item required for the business purpose of the system? Explain.
Yes. The data items are required to support the business purpose of the system, which is to identify taxpayers who represent a potential danger to the IRS and/or IRS Employee.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Information provided by the employee is verified through IDRS and the IRS Discovery Directory by the OEP staff. TIGTA provides the initial data. TIGTA agents investigate all complaints of IRS employees relating to assaults and threats. The Agency relies on TIGTA's Special Agents to verify data collected from sources other than IRS records. Information received by the state agencies is verified by the IRS Disclosure Office.

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

6. Generally, how will data be retrieved by the user?
Data will be retrieved by the user performing queries against the database. The case number is used to retrieve data, as it is the only unique identifier for EPS purposes.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. The case number is used to retrieve data, as it is the only unique identifier for EPS purposes. The taxpayer's name or SSN can also be used, but they are not always a unique identifier for EPS purposes.

Note: There are taxpayers with more than one case in EPS.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Authorized access is granted to the OEP Staff and Chief, OEP.

Role: OEP Staff
Permission: Read and write access to all data in the application and database.

Role: Chief, OEP
Permission: Reviews reports of user activities in the application.

Role: Developers
Permission: Access to the application source code on the development system to manage the EPS application.

Role: System Administrators
Permission: Full access to the application server to administer the operating system.

Role: Database Administrators
Permission: Full access to the database server to administer the EPS database management system.

Role: GAO and TIGTA Audit
Permission: Limited access for auditing purposes.

Note: Contractors do not have access to the system.

9. How is access to the data by a user determined and by whom?
The Chief, OEP determines who has access to the system. Only OEP employees with authorized access are granted access to the data. Online Form 5081 is required for all users.

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. No other IRS systems provide, receive, or share data in the 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?
Yes. Data in the EPS database is received from TIGTA and various state government agencies. EPS receives data from TIGTA through an interface. TIGTA uses the Secure File Transfer Protocol (SFTP) to send data to EPS. An Information Security Agreement (ISA) is in place between TIGTA and IRS entitled, Interconnection Security Agreement between Treasury Inspector General for Tax Administration (TIGTA) and Internal Revenue Service (IRS) In Support of Network Integration, June 23, 2008. Data in the EPS database is received from various state government agencies; however, the data is shared outside of the EPS database through hard-copy documentation. The IRS Disclosure Office handles all distribution of EPS data as required in IRC §6103(c).

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
The records of taxpayers not meeting established criteria are moved to the EPS Archive, where they remain for 5 years. At 5 years, the records are automatically permanently removed from the Archive. These retention procedures are per the advice of the Office of Chief Counsel under Manual Transmittal (10)-42, Item 17 – Miscellaneous Information Files (Threats and Protection), which is now IRM 1.15.12-1, Item 17. EPS records retention, however, will be specifically cited in Internal Revenue Manual (IRM) 1.15.22, which is currently under revision.

14. Will this system use technology in a new way?
No. This 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.
Yes. This system will be used to identify or locate individuals or groups by ID, address and data in remarks fields. The purpose is to protect IRS employees dealing with potentially dangerous/cautionary taxpayers.

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?
Yes. The PDT & CAU indicators notify employees of potential dangers that may arise through taxpayer contact. The employees decide how to work the case using IRM procedures such as IRM 5.1.3.1 and IRM 4.2.1.2. (“Procedures for handling PDT coded cases” and “Request for Armed Escort”).

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
No. The affected parties (Taxpayers) cannot respond to a negative determination.

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

View other PIAs on IRS.gov