Office of Tax Shelter Analysis Application (OTSA) – Privacy Impact Assessment (PIA)

PIA Approval Date: April 20, 2009

System of Records Notice (SORN):
- Treasury/IRS 42.021-- Compliance Programs and Project Files
- Treasury/IRS 42.001-- Examination Administrative Files
- Treasury/IRS 42.008-- Audit Information Management System
- Treasury/IRS 34.037-- IRS Audit Trail and Security Records System

System Overview
OTSA is a database system that supports the analysis of tax shelter activity by storing and providing user access to tax shelter disclosure information. The application supports the Office of Tax Shelter Analysis within the IRS Large and Mid-Size Business (LMSB) Business Unit. The application will be used by IRS employees with tax shelter examination duties to analyze tax shelter data and create reports.

Most of the data stored in the OTSA database consists of taxpayer submissions of the Reportable Transaction Disclosure Statement form (i.e., Form 8886). A transaction includes all of the factual elements relevant to the expected tax treatment of any investment, entity, plan, or arrangement, and it includes any series of steps carried out as part of a plan.

Data in the System

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

A. Taxpayer
- Taxpayer Name/Company Name
- Taxpayer Identification Number (TIN)
- Address

B. Employee
- User's Location
- SEID
- Permission Level

C. Audit Trail Information
- Employee activity including logon is recorded in the Audit Trail log, which includes the following fields:
  - Type of event / activity regarding the application
  - Date of event
  - Time of event

D. Other
- Name of other related parties*
- Other identifying information about other related parties including but not limited to the following:
  - TIN
  - Address

* "Other related parties" includes parties through which the tax shelter is established. This could refer to an individual, a company, or even a tax exempt organization but does not include the individuals reporting tax shelter violations on the anonymous hotline established for this purpose.

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

A. IRS – There is no IRS information obtained from files, databases, individuals or any other sources.

B. Taxpayer – Taxpayer information is drawn from e-filing Form 8886, Reportable Transaction Disclosure Statement, which is collected directly from the taxpayer. This form provides the following information to OTSA:
- Name
- TIN
- Address

C. Employee – No information is collected directly from the Employee. The information about the employee such as employee location is taken from the audit trail.

D. Other Federal Agencies – No information is obtained from other Federal Agencies.

E. State and Local Agencies – No information is obtained from State and Local Agencies.

F. Other Third Party Sources – Information is collected from the anonymous hotline set up to collect tips about illegal tax shelters. This information might include Personally Identifiable Information (PII) about a taxpayer/taxpaying entity, however the caller's PII is never collected.

3. Is each data item required for the business purpose of the system? Explain.
Yes. Each data element is collected to populate forms related to tax shelter activity.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Quality assurance optical character software is used to support the accuracy of data. Data is not submitted into the system until this software program has run. Additionally, as part of the data input process, data is checked based on the parameters of a field. For example, if an entry in the TIN field does not contain 9 digits, the application alerts the user to this inconsistency.

5. Is there another source for the data? Explain how that source is or is not used.
There are no other sources than those that have previously been referenced in this document.

6. Generally, how will data be retrieved by the user?
Data can be queried and retrieved by virtually any data element.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. The data is retrievable by a personal identifier (e.g., TIN). The ability to access data by a personal identifier is controlled by the SEID network logon procedure. The data retrieval is subject to audit and logging.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
A user's role is determined by the Group Manager of the OTSA group when he approves the OL5081. Only members of the OTSA group have access to the application. OTSA users are IRS personnel, who are agents, analysts, and field personnel, that have tax shelter examination duties and are located all across the United States. Contractors do not have access to the OTSA application.

9. How is access to the data by a user determined and by whom?
Access to the data is determined by the OTSA group manager who has the final approving authority. This access is governed by the rule of least privilege. The Online 5081 process is used for all users (i.e., IRS employees are the only users).

The OL5081 (Online 5081) is used to document access requests, modifications, and terminations for all types of users, including System Administrators. When a new user needs access to IRS systems or applications, the user's manager or designated official, completes an OL5081 requesting access for the new user. OL5081 is an online form, which includes information, such as the name of the system or application, type of access, and the manager's signature approving authorization of access. The completed OL5081 is submitted to the Security or User Administrator, who assigns a user ID and an initial password. Before access is granted, the user is required to digitally sign OL5081 acknowledging his/her security responsibilities when using the system.

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. There is no data shared data from 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. There will be no shared data received or provided by any other agencies.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
The data retention for the electronic data will be the same as the paper filed source documents. The retention schedule for the documents has been established as 2 years after the processing date to retire to Federal Records Center and 7 years after the processing year to destroy. All electronic data is scheduled for destruction in accordance with IRM 1.15.29 *Records Management – Records Control Schedule for Tax Administration*.

In addition, at the present time storage capacity is adequate for all data. In the future if storage becomes an issue the data will be archived to offsite media such as CD or tape.

14. Will this system use technology in a new way?
No. OTSA 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. OTSA will be used to see if taxpayers warrant further examination activity. Hence, the identity and location of those taxpayers is essential and is used only to support the business purpose of the system.

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. However, monitoring is not in real time. The data stored in the system is historical. For example, a user could find a taxpayer's tax shelter history for the past 4 years, but would not be able to obtain completely current information. This supports the business purpose of the system because in order to analyze tax shelter cases historical data is needed to observe trends in tax shelter activity over time.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.
No. Tax shelter laws preclude disparate treatment from occurring, and the system by design does not treat users or stakeholders differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. Any tax or penalty determination made in part or entirely by any data derived from the OTSA database can be appealed or taken to courts through existing procedures for any tax dispute.

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

View other PIAs on Irs.gov