Selection and Workload Classification Component – 1 (SWC C– 1) – Privacy Impact Assessment

PIA Date – Feb. 27, 2009

<u>**System Overview**</u>
The Selection and Workload Classification Component–1 (SWC C–1) is an IRS application that has been categorized as a Minor Application. SWC C–1 will reside on a Sun Solaris platform at the Enterprise Computing Center-Memphis (ECC–MEM). The primary document types to be handled are Tax Shelter disclosure documents such as Forms 8886 and 8918. These Tax Shelter documents are being scanned by Large and Mid-Size Business LMSB at the Ogden, Utah Campus. After the documents are scanned, they are placed in an Oracle database residing on Enterprise Operations controlled servers at the Ogden Campus. The Enterprise Architecture recommended Commercial off the Shelf (COTS) tool for document and content management is Documentum™, which is what SWC C–1 will employ to manipulate and analyze the Tax Shelter documents.

<u>**Systems of Records Notice (SORN):**</u>
- IRS 42.001 – Exam Administrative Files
- IRS 42.021 – Compliance Programs and Project Files
- IRS 34.037 – IRS Audit Trail and Security Records System

<u>**Data in the System**</u>

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

A. Taxpayer:
- Form 8886
- Name
- Address
- Taxpayer Identification Number (TIN)
- Form 8264/8918
- Name
- Address
- Taxpayer Identification Number (TIN)
- Phone Number
- Lead Development Center (LDC)
- Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Addresses
- Doing Business As (DBA)
- Form SS4
- Employer identification number (EIN)
- Executor Name
- Address
- Form 3520
- TIN
- Name
- EIN
- Address

- Form 3520A
- EIN
- Address
- SSN
- Phone Number

B. Employee
- Audit trails of employee logins and access which includes a unique user name and password

C. Audit Trail Information
- Users' log-in information which includes a unique user name and password
- Any action taken by the user
- Time and date of the activity

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.
A. IRS
- Integrated Data Retrieval System (IDRS)
- Name
- Address
- TIN
- LDC
- Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Addresses
- Doing Business As (DBA)

B. Taxpayer
- Name
- SSN
- TIN
- Addresses
- Phone Numbers
- DBA

C. Employee
- Login information which includes a unique user name and password

D. Other Federal Agencies
- Department Of Justice (DOJ) injunction information provided via e-mails

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data items are necessary to identify abusive transactions and the promoters/material advisors, and taxpayers who participate in the transaction.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Taxpayer self-discloses involvement in transaction; data items are required by a certain time. Taxpayers may be contacted for timeliness and completeness. If required, SWC-C1 staff mails a letter to the taxpayer asking them to provide complete information. This takes place outside the system.

5. Is there another source for the data? Explain how that source is or is not used.
No. There is not another source for the data that has not been previously identified.

6. Generally, how will data be retrieved by the user?
The data is generally retrieved via a query or report by logging onto the Webtop client of Documentum.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. The data is retrievable by TIN and/or name.

Access to the Data

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

> **Role:** End-Users (technical advisors and Revenue Agents)
> **Permission:** Read; write; change; delete

> **Role:** Application Administrators
> **Permission:** Read; write; change; delete

9. How is access to the data by a user determined and by whom?
Access to the data is determined by the user's manager based on a user's position and need-to-know. The user's manager will request a user to be added. They must use the Online (OL) 5081 process. This form will contain information on the level of access to be granted to the requesting user. Approval will have to be granted by the user's manager and the SWC C–1 application administrator before the account is created and the access level granted.

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.
Yes, SWC C–1 receives information from IDRS, REVEAL and Lead Development Center (LDC). The system does not share with or provide any data to any other system. This application is not directly linked with any other system. The system will not directly make any updates.

- IDRS provides the group control information (Primary Business Code, Secondary Business Code and Employee Group Code) as well as the BOD code.

- REVEAL – Criminal Investigation Division System provides information from the Forms SS4, 3520 and 3520A.

- The LDC data comprises information on abusive taxation promoter leads received through various sources. The LDC data provided includes information on the promoter identified in the lead, lead process tracking, and approved investigation tracking information.

- See questions #1 and 2 for data elements.

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

IDRS:
- Certification & Accreditation (C&A) – Authority to Operate (ATO) received on May 18, 2006, expires May 18, 2009
- Privacy Impact Assessment (PIA) – November 6, 2008, expires November 6, 2011

LDC:
- There is no PIA or ATO for LDC.

12. Will other agencies provide, receive, or share data in any form with this system?
No. The data in the system is IRS data and will not be shared 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. A SF115 will be initiated to have all electronic data scheduled for destruction in accordance with IRM 1.15.29 Records Management – Records Control Schedule for Tax Administration.

14. Will this system use technology in a new way?
No. SWC C–1 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. SWC C–1 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. User transactions will be reviewed by the Audit Trail logs. The system will utilize the MITS 5081 process for access to the system. For the Forms 8264\8918 and 8886, the system will only allow IRS employees to monitor whether or not a taxpayer filed the proper form. The business purpose is to determine the level of compliance with the law requiring the filing of the forms. IRS employees will also review the transactions that are described on the forms. Subsequent actions might be taken. However, they are done outside the system.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. The purpose of the system is to improve efficiency of employees dealing with tax shelters.

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 in the SWC C–1 database can be appealed or taken to court 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?
Yes the system is web-based. It utilizes the Webtop client of Documentum. The system keeps track of the log–-in information (user SEID, date and login time/logout time) The system also utilizes the IRS Secure firewall. The login screen can create a persistent cookie to save credentials.

View other PIAs on IRS.gov