

YK1 Readiness (YK1) – Privacy Impact Assessment

PIA Approval Date – Jan. 14, 2010

System Overview

The YK1 Readiness system is a Research, Analysis and Statistics (RAS) development prototype effort capable of graphically displaying connections between entities suspected of engaging in abusive tax avoidance transactions. YK1 Readiness is an interactive tool which discovers and explores tax entities and their relationships. The YK1 system is normally accessed through Microsoft Windows workstations over the Internal Revenue Service (IRS) local area network (LAN). Taxpayer data is collected from taxpayer forms including: K-1, 1040, 1041, 1065, 1120, 1120F, 1120FSC, 1120H, 1120L, 1120ND, 1120P, 1120PC, 1120REIT, 1120RIC, 1120S, 1120SF, 5227, 5500, and Form 990. This data includes Social Security number (SSN), employer identification number (EIN) and taxpayer identification number (TIN) information.

Systems of Records Notice (SORN):

- IRS 42.021-- Compliance Programs and Project Files

Data in the System

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

- A. Taxpayer – Taxpayer data available in YK1 includes extracts from the following forms: K-1, 1040, 1041, 1065, 1120, 1120F, 1120FSC, 1120H, 1120L, 1120ND, 1120P, 1120PC, 1120REIT, 1120RIC, 1120S, 1120SF, 5227, 5500, Form 990 – Return of an Organization Exempt from Income Tax File, Split-Interest Trust Information Form 5227, K1, and Annual Return/Report of Employee Benefit Plan Form 5500. On the first pass, the extracts include examination of individuals with either 1) a total positive income (TPI) greater than or equal to \$250,000 or 2) who have filed a Schedule E. On the second pass, YK1 examines individuals who have received a K-1 but who were not included in the first pass (possibly because their TPI was less than \$250,000 or because they did not file a Schedule E despite receiving a K-1). A description of each data element is available in the YK1 Link Analysis Tool Production Readiness Data Dictionary. This document is available upon request.
- B. Audit Trail Information – User Log-in ID and timestamp are captured in the audit trail log of the application. Future audit capabilities being developed include negative TIN checking and recursive analysis.
- C. Other – Data from the Large and Mid-Size Business (LMSB) Tax Haven Country List and Office of Tax Shelter Analysis Listed Transactions File. LMSB Corporate Parent/Subsidiary Relationship List is used by YK1 to identify how relationships exist between corporations.

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

- A. IRS – IRS data is obtained from the following forms: K-1, 1040, 1041, 1065, 1120, 1120F, 1120FSC, 1120H, 1120L, 1120ND, 1120P, 1120PC, 1120REIT, 1120RIC, 1120S, 1120SF, 5227, 5500, and Form 990.

- The TE/GE Extract tool identifies non–profit organizations that may be used as flow–through entities via data from forms including: Form 990 – Return of an Organization Exempt from Income Tax File, Split–Interest Trust Information Form 5227, Annual Return/Report of Employee Benefit Plan Form 5500.
- The Individual Return Transaction File Extract identifies entity and transactional information via data from various forms filed with Individual Return Transaction File – Form 1041.
- The LMSB Tax Haven Country List is a listing of nations that have relaxed banking standards that may shelter flow–through entities. Data from this list is used by YK1 to identify how relationships exist between corporations.
- Office of Tax Shelter Analysis (OTSA) Listed Transactions File provides YK1 with a listing of proscribed tax shelters defined as abusive by the IRS and the tax court.
- Data from the LMSB Corporate Parent/Subsidiary Relationship List provides YK1 with data that can be used to identify the nature of corporate structures

B. Taxpayer – Taxpayer name, address, telephone number, SSN, and completed line items on the tax return and any attached schedules as filed by the taxpayer or his representative are maintained within the system. This includes data in both electronically–submitted and paper–filed returns.

3. Is each data item required for the business purpose of the system? Explain.

Yes. The purpose of YK1 is to prototype a tool that can be used by IRS analysts, auditors and case–builders to examine tax entities and their relationships to identify areas of non–compliance in flow–through entities (Partnerships, S Corporations, Trusts, Employee Plans, and Individuals) and their beneficiaries. To achieve this mission, YK1 needs taxpayer information from files that contain the data elements that may indicate a flow–through entity. To identify these relationships, YK1 needs data on businesses, individuals, corporations, and non–profit organizations. YK1 has assessed the data required to achieve its mission and has determined that it is the minimum data necessary to achieve its mission and business purpose of identifying tax avoidance.

4. How will each data item be verified for accuracy, timeliness, and completeness?

YK1 does not verify extracts received for accuracy, timeliness, and completeness. YK1 utilizes IRS Masterfile extracts and data provided by the business units detailed above. YK1 relies on data owners to conduct accuracy, timeliness and completeness checks.

5. Is there another source for the data? Explain how that source is or is not used.

No. There are no other sources for the data in this system.

6. Generally, how will data be retrieved by the user?

Data is retrieved by TIN, EIN or SSN from a central server using an installed client over the IRS Intranet. Searching by TIN, EIN or SSN is only successful if a K–1 Form exists for the TIN, EIN or SSN. If the search is successful then a graph will be displayed otherwise the search will notify the user that the TIN, EIN or SSN was not found.

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

Yes. Data can be retrieved by TIN, EIN, or SSN.

Access to the Data

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

Role: Users – Case building analysts, auditors, and management designees in the following Business Units:

- Criminal Investigations (CI)
- Large and Mid–Size Business (LMSB)
- Small Business Self Employed (SBSE)
- Tax Exempt and Government Entities (TE/GE)
- Wage and Investment (W&I)
- Chief Counsel (CC)

Permission: need access to the data for the purposes of investigating tax shelters

Role: Developers, System and Database Administrators:

Permission: These individuals will have access to the system for the purposes of uploading extracts received and development

Role: Contractors

Permission: Contractors performing in the above roles may be given access to the data in the system. Access is granted through the same procedures by the Contract Officer's Technical Representative (COTR) on the project. Contractors accessing YK1 must have High–Risk clearances.

9. How is access to the data by a user determined and by whom?

All access credential requests are enforced through the Online 5081 process for granting permissions to systems and applications used by IRS personnel. A formal request is made through the User's, Developer's, or System/Database Administrator's management chain. Online 5081 forms are completed. Each request is evaluated by RAS management and a determination to grant access or deny access is made.

Once an individual has an YK1 account, they have direct access to data within the system. Access to data begins at an "entry node" determined by an auditor or analyst, or management designee. The "entry node" is the node where a SSN, EIN, or TIN is entered to draw a graph.

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. YK1 data extracts are provided to YK1 and this data is not shared with any other IRS system. YK1 is not connected to any other IRS system.

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

Not applicable. YK1 does not provide, receive, nor share data with other IRS systems.

12. Will other agencies provide, receive, or share data in any form with this system?

No, no other agencies will provide, receive or share data in any form with YK1.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

Records are maintained, administered and disposed of in accordance with the Internal Revenue Manual (IRM) 1.15.30, Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003, Item number 15, Investigative Files. Audit logs are maintained in compliance with IRM 10.8.3, Audit Logging Security Standards.

14. Will this system use technology in a new way?

Yes. The application provides a visualization of dollar transfers through flow-through entities. The system uses descriptive graph theory to visualize these relationships. YK1 combines previously unavailable multiple data sources within one searchable database. Previously, the work done by YK1 could have been done by analysts; however, the time, effort, and labor required to conduct large-scale analyses made the task nearly impossible.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.

Yes. Individuals and flow-through entities are identified as part of YK1. Flow-through entities do not pay taxes directly. Tax payments are often routed through other flow-through entities, ultimately ending in an individual tax return (Form 1040 variants). The purpose of this examination of flow-through entities' return data to individuals is to allow the IRS to identify potential abusive tax shelters and individuals that are linked to the abusive tax shelters.

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. YK1 will provide the capability to monitor individuals and groups with due cause; however, the monitoring of individuals and/or groups is not automated, but must be initiated by a tax analyst. The business purpose of this monitoring is to identify entities suspected of engaging in abusive tax avoidance transactions. Tax abuse shelters are reconstituted annually. Some individuals and some preparers join in a client/provider relationship to enable tax fraud at significant levels.

General unauthorized access (UNAX) is provided to all IRS employees and contractors to prevent unauthorized monitoring. Additionally, specific training is provided to employees and contractors to further inform them of proper procedures for monitoring individuals and groups. Additional controls to prevent unauthorized monitoring that will be implemented at a future date include negative TIN checking.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

Yes. Through the system's TPI and Schedule E analyses, YK1 will be used to automate examinations which currently are performed by hard copy investigations.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Yes. YK1 is an investigative tool to identify tax shelters. The system does not make a negative determination about an individual or business; rather, investigators monitoring YK1 data make determinations about individuals or businesses that may have a negative impact. The use of YK1 is limited to investigative purposes. Individuals can respond to any negative determination made which is supported through the use of YK1.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

Not applicable, the system is not web-based.

[View other PIAs on IRS.gov](#)