
A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10-Privacy Accountability and #21-Privacy Risk Management

Date of Submission: Apr. 3, 2013 PIA ID Number: 435

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

YK1 Readiness (YK1)

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Under 5,000

Members of the Public: Not Applicable

4. Responsible Parties:

N/A

5. General Business Purpose of System

The YK1 Readiness system a Research, Analysis and Statistics (RAS) development prototype effort capable of graphically displaying connections between entities suspected of engaging in abusive tax avoidance transactions. The focus of the system is a structure known as a flow-through entity such as a partnership (Form 1065), Subchapter S corporation (Form 1120S) or trust (Form 1041). YK1 Readiness is an interactive tool which discovers and explores tax entities and their relationships. The application draws graphs of nodes and links. Nodes generally represent tax returns for flow-through, corporations, individuals and Tax Exempt and Government Entities (TE/GE). Links between the nodes reflect Schedule K-1 activity and parent-subsidary or husband-wife relationships. Schedule K-1 activity involves reported income, and credits and deductions to the partners, shareholders and beneficiaries involved. Nodes and links can be queried to provide more detailed information and the graphs can be expanded by iteratively pursuing nodes of interest. The common thread for these flow-through entities is Schedule K-1 filings. These filings link flow-through entities, creating tiered relationships which readily lend themselves to questionable and abusive schemes that can hide, offset or otherwise manipulate taxable income. The YK1 application, developed in Java utilizing the yFiles library from yWorks, is an interactive customized visualization tool. It is Intranet-based and employs an Oracle database in a Sun Microsystems hardware environment running the Solaris operating system. 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.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact *Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 01/14/2010

6b. If Yes, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
- System is undergoing Security Assessment and Authorization Yes

6c. State any changes that have occurred to the system since the last PIA

No changes

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23-PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes**8a. If No, what types of information does the system collect, display, store, maintain or disseminate?****9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:**

Taxpayers/Public/Tax Systems	<u>Yes</u>
Employees/Personnel/HR Systems	<u>No</u>
Other	<u>No</u>

Other Source: _____

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: Yes

No Other PII Records found.

10a. Briefly describe the PII available in the system referred to in question 10 above.

Name Address Elements on partnership, s-corporation, certain exempt organization, and trust tax forms

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.**10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)**

SSNs are permissible from Internal Revenue Code (IRC) 6109, "Identifying Numbers" which requires individual taxpayers to include their SSNs on their income tax returns. Additional information can be found at: <http://www.law.cornell.edu/uscode/text/26/6109>

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

None.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

SSNs are the primary key, used by auditors and analysts to tie together a few to thousands of tax forms relating to a tax case. The replacement of this identifier with a masked ID would be impractical.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Below are the elements that are collected in the audit record. "SQL_TEXT" is the text of the query that is delivered to the database. Session id, "TIMESTAMP" db_user os_user userhost client_id econtext_id ext_name object_schema object_name policy_name "SCN" SQL_TEXT1 SQL_TEXT2 SQL_TEXT3 SQL_TEXT4 SQL_TEXT5 SQL_TEXT6 SQL_TEXT7 SQL_TEXT8 sql_bind comment\$text statement_type extended_timestamp proxy_sessionid global_uid instance_number os_process transactionid statementid entryid processed_ind

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If Yes, the system(s) are listed below:

System Name Current PIA? PIA Approval Date SA & A? Authorization Date

No

No

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): No

g. Other: No If Yes, specify:

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

This application presents tax form information for partnerships, s-corporations, trusts, and certain tax exempt forms. These forms contain taxpayer identification. The taxpayer identifiers, ssn, address, name, etc are used for analysis and primary and foreign key purposes in a database for data recall and analysis.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	<u>Yes</u>
To provide taxpayer services	<u>No</u>
To collect demographic data	<u>No</u>
For employee purposes	<u>No</u>

If other, what is the use?

Other: No

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14-Privacy Notice and #19-Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) Yes

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	Yes	Congress, if requested	No
State and local agency (-ies)	No		
Third party sources	No		
Other:	No		

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	<i>If other, specify:</i> _____

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15-Consent and #18-Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

18a. If Yes, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

<u>Form Number</u>	<u>Form Name</u>
1040	Individual Tax Return
1041	Trust
K1	Schedule K1
1065	Partnership
1120 (various)	Corporation
5227	Split Interest Trust

5500 Employee Benefit Plan
990 Exempt Organization Return

20b. If No, how was consent granted?

Written consent _____
Website Opt In or Out option _____
Published System of Records Notice in the Federal Register _____
Other: _____

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9-Privacy as Part of the Development Life Cycle, #11-Privacy Assurance, #12-Privacy Education and Training, #17-PII Data Quality, #20-Safeguards and #22-Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Write</u>
Developers		<u>Read Write</u>
Contractors:	<u>Yes</u>	
Contractor Users		<u>No Access</u>
Contractor System Administrators		<u>Read Write</u>
Contractor Developers		<u>Read Write</u>
Other:	<u>No</u>	

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation? Yes

23. How is access to the PII determined and by whom?

An individual auditor/analyst will request access via the IRS 5081 system. That request is forwarded to the individual's manager. If the manager approves, that request is then forwarded to the administrators of the system.

24. How will each data element of SBU/PII 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 business units. YK1 relies on data owners to conduct accuracy, timeliness and completeness checks.

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

25a. If Yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

YK1 data is approved for destruction 16 years after processing year or when no longer needed for operational purposes, whichever is later (Job No. N1-58-09-86, approved 4/22/10). These disposition instructions will be included in IRS Document 12990 under Records Control Schedule 27 for Compliance Research, item 53 when next updated/published. Records are retained for this long to capture any recycling of tax evasion strategies for flow through-based tax schemes. Periodically, untoward actors will recycle schemes and we have found that keeping past evidence assists in new investigations/audits. Often, the same individuals are involved.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

We currently retain records for 10 years. We retain records this long in order to capture any recycling of tax evasion strategies for flow through-based tax schemes. Periodically, untoward actors will recycle schemes and we have found that keeping past evidence assists in new investigations/audits. Often, the same individuals are involved.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

YK1 is a FISMA-reportable IRS application adhering to NIST guidelines and procedures. All access is secured by a multi-level review. Individual employees undergo UNAX training and are held to statutory requirements for access to taxpayer information.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

The YK1 application server reside in the Martinsburg Computing Facility (MCC). YK1 is not a mobile application and transition (updates) are handled by appropriate systems administrators and database administrators.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

YK1 contains an audit system (ORACLE Fine-Grain Auditing) that is maintained by systems personnel. The IRS 5081 system is utilized for all users, both application users and administrators.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 – IT Security, Live Data Protection Policy? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21-Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

32a. If Yes to any of the above, please describe:

N/A

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