

Date of Approval: **March 19, 2019**

PIA ID Number: **3832**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

yK1 Readiness, yK1

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

PCLIA 1641, YK1 Readiness

What is the approval date of the most recent PCLIA?

2/25/2016

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Research, Applied Analytics and Statistics (RAAS)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The yK1 Readiness is an application developed in the Research, Applied Analytics and Statistics (RAAS) division that graphically displays connections between flow-through entities such as partnerships (form 1065), subchapter S corporations (form 1120S), trusts (form 1041), and other taxable owners (e.g., individuals filing 1040, corporations filing 1120, etc.). The connections (or relationships) between entities is based on schedule K-1 and can be deeply nested. Such nested structures can be difficult to understand and analyze based solely on an entity's tax return. Further, such tiered relationships can easily lend themselves to questionable and potentially abusive schemes that can hide, offset or otherwise manipulate taxable income. This application helps examiners and researchers visually understand and analyze the complete structure of an entity. As the primary Internal Revenue Service (IRS) tool to examine and analyze flow-through entities, this application benefits users from Large Business and International (LB&I), Small Business Self Employed (SBSE), Chief Counsel, and other IRS divisions.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

The IRS collects tax returns of individuals (AKA taxpayers). As such, the identification of taxpayers is done with the use of SSNs.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed. There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Protected Information Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant)

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

Examination of flow-through tax entities is the primary goal of users of this application. Because taxpayer data uses Social Security Numbers (SSNs), Employer Identification Numbers (EINs), Individual Taxpayer Identification Number (ITINs), etc. as the means of identifying and relating entities, it is necessary for the application to use these tax identification numbers. Also, these tax identification numbers are used as primary keys in a database from where this information is used for recall and analysis. This application only presents information that is found in tax forms that are filed with the IRS.

How is the SBU/PII verified for accuracy, timeliness and completion?

yK1 does not verify extracts of tax data received for accuracy, timeliness, and completeness. yK1 uses IRS Masterfile extracts and data provided by business units. yK1 relies on data owners to conduct accuracy, timeliness, and completeness checks. Furthermore, yK1 users follow approved procedures as stipulated in their organization's Internal Revenue Manual (IRM).

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 42.021 Compliance Programs and Projects Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Individual Masterfile

Current PCLIA: Yes

Approval Date: 2/28/2017

SA&A: Yes

ATO/IATO Date: 10/25/2018

System Name: LB& I Datamart

Current PCLIA: No

SA&A: No

System Name: Information Returns Processing
Current PCLIA: Yes
Approval Date: 9/20/2018
SA&A: No

System Name: Business Masterfile
Current PCLIA: Yes
Approval Date: 8/27/2018
SA&A: Yes
ATO/IATO Date: 1/29/2018

System Name: Return Information Control System (RICS) Database
Current PCLIA: Yes
Approval Date: 2/19/2019
SA&A: Yes
ATO/IATO Date: 7/11/2018

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1040 Form Name: U.S. Individual Income Tax Return

Form Number: 1120 Form Name: U.S. Corporation Income Tax Return

Form Number: 1120S Form Name: U.S. Income Tax Return for an S Corporation

Form Number: 1065 Form Name: Return of Partnership Income

Form Number: 1041 Form Name: U.S. Income Tax Return for Estates and Trusts

Form Number: 990 Form Name: Return of Organization Exempt From Income Tax

Form Number: 5500 Form Name: Returns for employee benefit plans

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: U.S. Government Accountability Office (GAO)

Transmission Method: Application Access

ISA/MOU No

Identify the authority

IRC § 6103(i)(8)(B) permits U.S. Government Accountability Office (GAO) access to any returns or return information obtained by a federal agency for use in any agency program or activity to the extent necessary in auditing such program or activity. Access is permitted pursuant to IRM 11.2.3.3.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

Application Access

For what purpose?

Audit

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

Yes

Identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Any contractor passing valid checks
Transmission Method: Application Access
ISA/MOU No

Identify the authority

IRS contractors working on projects requiring access to yK1 are granted access if all of the following conditions are met: a. A completed background investigation b. Submission of a Minimum Background Investigation (MBI) report c. Request from contractor's manager justifying reason(s) for access d. Completion of online 5081 request e. Statement indicating specific term and id of contract under which access is requested.

For what purpose?

No

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

No

Explain:

The contract does not include a 6103 clause. However, it does include IR1052.224-9009 (IRS INFORMATION PROTECTION AND SECURITY AWARENESS TRAINING REQUIREMENTS) and IR1052.239-9007 (ACCESS, USE OR OPERATION OF IRS INFORMATION TECHNOLOGY (IT) SYSTEMS BY CONTRACTORS) clauses.

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

The information is not collected directly from individuals. The information collected as part of the application is the information obtained from various IRS databases and files, which in turn are tax form filed by tax entities. Those data sources (and related forms) provide Privacy Act Notice, consent and due process to individuals. Due process is provided pursuant to 5 USC. Publication 1 "Your Rights as a Taxpayer" explains the rights of the taxpayer, which includes the right to challenge the IRS' position and be heard; and the right to appeal an IRS decision in an independent forum.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Contractor Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Write

How is access to SBU/PII determined and by whom?

yK1 is not accessible by the public. Request for access are made only via the Online (OL) Form 5081 system. This request has to be approved by the potential user's manager based on a user's position and need-to-know. If approved, the request is then forwarded to the administrators of the system for the creation of a new user id and password. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. The employee's access will be terminated once they no longer require access to the Database. Deletion from the active access role is also performed through the OL5081.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

yK1 data is approved for destruction 16 years after processing year or when no longer needed for operational purposes, whichever is later. 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.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

1/19/2019

Describe the system's audit trail.

Every time a yK1 user accesses the application for investigating a tax entity, the following information about the request is collected: 1. The username of the user 2. The time of access 3. The Tax Identification Number (TIN) of the entity being investigated 4. TINs of all the tax entities returned as a result of the access 5. All system-level information that went into processing the request

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

yK1 follows the following testing procedure: first a code review is done by the team of developers; next once the code is in place the application is tested first by the developers and then by the Subject Matter Expert (SME) who makes sure the application responds as expected, data wise.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

No

Accounting of Disclosures risk noted. Contact Disclosure to develop an accounting of disclosures. Explain steps taken to develop accounting of disclosures process.

The contract does not include a 6103 clause. However, it does include IR1052.224-9009 (IRS INFORMATION PROTECTION AND SECURITY AWARENESS TRAINING REQUIREMENTS) and IR1052.239-9007 (ACCESS, USE OR OPERATION OF IRS INFORMATION TECHNOLOGY (IT) SYSTEMS BY CONTRACTORS) clauses.