

NOTE: The following reflects the information entered in the PIAMS website.

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 Approval: 6/2/14

PIA ID Number: **735**

1. What type of system is this? Legacy

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

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

Returns Inventory and Classification System, RICS

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: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: 100,000 - 1,000,000

4. Responsible Parties:

N/A

5. General Business Purpose of System

RICS is Tax Exempt & Government Entities (TE/GE) primary tool for examining the level of tax filing compliance from its customers. RICS allows access to tax filing data related to filing, processing, and posting of returns. RICS also provides automatic sampling, criteria for audits, and the tracking of audit results. TE/GE uses RICS to study specific filer samples to determine the level of compliance of individual customer groups. Since most customer groups are too large to study each filer, RICS provides statistically sound sampling allowing TE/GE to make assessments about a particular group by studying a much smaller subset of filers. The RICS application consists of five components, the mainframe, (GSS-21 ECC-MTB System domain), the web-based module for RICS (GSS-24 ECC-DET System domain) and the EDAS_XRDB & EDW_XRDB (XRDB Oracle Database located in Detroit, MI, GSS-24 ECC-MTB System Domain), RICS Hummingbird BI Query server (located in Martinsburg, WV and resides on the GSS-30 System) and the Microsoft Access database (located in Philadelphia, PA and resides on the GSS-30 System) The XRDB functionality is used primarily by the RICS application as a source for EO-MeF data (electronically filed Forms 990, 990EZ, 990PF, and their related schedules). RICS allows the selection of tax forms with any combination of characteristics that may suggest a high potential for filing errors. All selection criteria results can be revised quickly and viewed on the screen or printed. Since RICS provides PDF versions of tax returns, RICS users are able to eliminate long delays waiting for ordered hardcopy returns from service center files. These selections through RICS also allow the user to group forms into categories, allowing easy assignment based on the project being worked. Due process is provided pursuant to 26 USC

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: 9/20/2011 12:00:00 AM

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) Yes
- System is undergoing Security Assessment and Authorization No

10a. What is the business purpose for collecting and using the SSN?

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.)

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

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

Describe the PII available in the system referred to in question 10 above.

The taxpayer information available is primarily on organizational and business taxpayers, with the exception of individual taxpayer data available on a limited number of forms (which includes individual information. The list of forms is shown below. This information includes data elements from the following forms: WebRICS Forms and Information Form 5500- Annual Report of Employee Benefit Plan Name of Plan Sponsor (with Employer Identification Number (EIN)) Name of Plan Administrator (with EIN) Preparer's Information and Preparer Tax Identification Number (PTIN) Form 990 (including Schedule B) Return of Organization Exempt from Income Tax: Contributors' names Contributors' mailing addresses Contributors' zip codes Form 5330 Return of Excise Taxes Related to Employee Benefit Plan: Name of filer Filer's identifying Number (EIN) Address of Filer, Filer telephone number Schedule A – Form 990 Name of Employees Preparer's Information and PTIN All other data represents businesses organizations and pension plans. DB2 Database Forms and Information: 11C 1041 1120L 5227 720 1041A 1120ND 5330 730 1042 1120PC 5500 940/940EZ 1065 1120POL 5500EZ 941 1065B 1120REIT 8038 943 1096 1120RIC 8050 944 1120 1120S 8703 945 1120A 1120SF 8328 990C 1120C 2290 8804 990/990EZ 1120F 5500SF 8871 990PF 1120FSC 4626 8872 990T 1120H 4720 W2 990N 8038B 038G 8038GC 8038CP 8038TC The above forms (including applicable schedules) are contained within the EDAS_XRDB and EDW_XRDB database of the RICS system and may contain the following elements: Address Name Phone Preparer TIN (PTN)

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.

RICS maintains an audit plan that outlines the required steps. WebRICS Audit Trail: Date Time Username Returns printed DB2 Database Fields - Audit Trail: EIN Master File Code Plan number Mode code Document code Exam code Tax period Non Exam Date Condition code Org code Creation Date Org generated code Document Locator Number Project code Error code Purpose code File name Seed text Form count Source code Select Code Status code Issue codes User Identification (ID) code Creation Time

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**

BMF Yes No

EARP No No

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): No

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

g. Other: No

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.

RICS primarily is used to identify entities for which RICS has address information which is used to locate that organization or business. RICS also contains a small portion of data on individuals. This access is used exclusively for examination purposes. The availability of each data item within RICS allows for an easier and faster method to examine the level of compliance from its customers. The selection of data through RICS allows the user to group forms into categories, allowing easy assignment based on the project being worked. The data can be used to verify consistency of information between filings and other more complicated trend analysis. RICS is needed as a research tool to provide for consistency of information and trend 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 Yes

To provide taxpayer services Yes

To collect demographic data No

For employee purposes No

Other: No

If other, what is the use?

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.) No

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)			
State and local agency (-ies)			
Third party sources			
Other:			

** 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:	_____	_____

If other, specify:

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.

No forms found.

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 Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></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?

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

TE/GE puts restrictions on and determines access based on user role. Users request this access through OL5081. Users are only granted access to RICS as necessary to fulfill the duties of their role. Through the access control mechanisms employed, the application establishes appropriate division of responsibility and separation of duties to eliminate conflict of interest in the responsibilities and duties of individuals. The role-based access groups defined within the RICS application enforce the most restrictive set of rights/privileges or access needed by users to perform their tasks; thereby, enforcing least privileges. To clarify; an EO user only has access to EO data, and an EP user only has access to EP data. The second level is controlled on the BI Server which further restricts permissions based on roles.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

RICS receives data from various IRS systems which have their own verification process for data accuracy, timeliness, and completeness; therefore, RICS assumes that the data is accurate, timely, and complete when it is provided by the other systems

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.

RICS maintains in excess of ten years of TE/GE form data. RICS data and associated records are scheduled under a variety of disposition authorities in accordance with Internal Revenue Manual (IRM)/Records Control Schedule (RCS) 1.15.24 for TE/GE. The Records Office is currently working with TE/GE to update 1.15.24, including the identification and scheduling of electronic systems in a manner that clearly identifies system inputs, outputs, master data files, and system documentation. As part of this scheduling initiative, the Records Office asks TE/GE assistance to better outline the identification and associated dispositions for RICS in those terms, for future

publication in RCS Document 12990 under RCS 24 specific to this system (all former RCS IRMs 1.15.8-37 are transitioning from an IRM publication format to consolidated publication in Document 12990). The Records Office also recommends the consideration of a DoD 5015-compliant recordkeeping system to appropriately affect RICS records destruction/deletion.

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.

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

The RICS system utilizes the Enterprise File Transfer Utility (EFTU) to encrypt data transferred between the interconnected applications. Data at rest is protected using the Guardian Edge Removable Storage (GERS) encryption solution. Both are recognized IRS standards for protecting data.

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

The RICS system utilizes the Enterprise File Transfer Utility (EFTU) to encrypt data transferred between the interconnected applications. Data at rest is protected using the Guardian Edge Removable Storage (GERS) encryption solution. Both are recognized IRS standards for protecting data.

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.

Annual Enterprise Continuous Monitoring (eCM) activities take place to evaluate a subset of security controls associated with the system.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate*)? Yes

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

5/21/2013 12:00:00 AM

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.

Treasury/IRS 24.046 IMF CADE

Treasury/IRS 34.037 IRS Audit Trail and Security Records System

Treasury/IRS 50.222 Tax Exempt/Government Entities (TEGE) Case Management

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:

NA