Report Generation Software (RGS) – Privacy Impact Assessment

PIA Approval Date: April 23, 2009

Requested Operational Date: April 1, 2009

System Overview

Report Generation Software (RGS) allows key steps involving complex tax calculations to be accomplished more accurately and efficiently through the use of automation. RGS is used to prepare examination reports, propose adjustments, generate correspondence and work papers, and complete case closing documents. It also provides access to Return Transaction File (RTF) data for cases that are being audited, allows the automated closure of cases on the Audit Information Management System (AIMS), and provides for long and short closures. RGS provides taxpayers an accurate, legible, and easily understood audit report where the tax law and interest computations have been uniformly applied.

System of Records Notices (SORN):

- Treasury/IRS 34.037 IRS Audit Trail and Security Records
- Treasury/IRS 42.001 Exam Administrative Files

Data in the System

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

A. Taxpayer – RGS contains primary and secondary Taxpayer Identification Numbers (TIN); primary and secondary taxpayer name, contact information (current and previous), phone, fax and address; and primary and secondary taxpayer return information.

B. Employee – RGS obtains name, work address, work phone number and badge ID number / user login information of employees who use the application. This information is keyed in by the employee when setting up an examination file (Same as 2C below).

C. Audit Trail Information – RGS contains user login information. Records for the Case History application within RGS are date-stamped with pre-audit, examination, report and case closing information.

The audit trail for contractors is the same as it is for employees. Audit logs are maintained which can be used to track
account access.

D. Other - RGS contains all information obtained from interviews, adjustments, workpapers, compliance evaluation and 5344 (the closing document).

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

A. IRS – Entities, tax module, tax return information related data fields are obtained from files and databases from the following systems: Dependent Database (DDB), Corporate Files On Line (CFOL), Return Transaction File (RTF), AIMS, Correspondence Examination Automation Support (CEAS) and Exam Operation Automation Database (EOAD).

B. Taxpayer – RGS does not obtain taxpayer data information directly from the taxpayer. Taxpayer data is obtained from files and databases listed in 2A. However the taxpayer may provide receipts, bank statements or other supporting documentation which would keyed in by the employee.

C. Employee – RGS obtains name, work address, work phone number and badge ID number of employees who use the application. This information is keyed in by the employee when setting up an examination file.

D. Other Third Party Sources – Information that could be obtained from third party sources includes Power of Attorney (POA), as well as information related to the case. This may include data obtained from bank statements or receipts, or employee benefit information, for example. The information is keyed in by the employee working the case.

3. Is each data item required for the business purpose of the system? Explain.
Yes. Each data item is used for the business purpose of the system.

RGS allows key steps involving complex tax calculations to be accomplished more accurately and efficiently through the use of automation. RGS is used to prepare examination reports, propose tax related adjustments, generate correspondence, and work papers, and complete case closing documents. It also provides access to Return Transaction File (RTF) data for cases that are being audited, allows the automated closure of cases on the Audit Information Management System (AIMS), and provides for the closure process via a Local Area Network (LAN).

RGS provides taxpayers an accurate, legible, and easily understood audit report where the tax law and interest computations have been uniformly applied.

4. How will each data item be verified for accuracy, timeliness, and completeness?
RGS has in place a number of mechanisms to validate input data. The application checks for:

- validity, completeness, and authenticity.
- validation on the type of information that is entered; for example, dollar amounts, numbers, letters;
- rules for input restrictions
- variance tool to validate the taxpayer math

Prior to a case being closed, a validation check is performed on the Form 5344 to verify that the information that has been entered is accurate. The information has to be validated and made accurate before the F5344 can be submitted and the case closed.

Another type of validation that occurs is validation against other values. That is, if one field has some value, then other fields can only have certain values.

The Revenue Agent Report is another form (a document that is sent to taxpayers) that is an output that is generated that has checks and balances based on tax laws and other factors.

The following explanations detail some of the input validations that are performed by the RGS application:

- Information can be manually entered into RGS by a user or downloaded from a server. The information is in the form of the tax return as originally filed.

- The user verifies the data by calculating a Variance. Variance calculates the return as entered and compares the results to the data entered in Return Setup. Any differences are displayed. Differences can be due to input errors or math errors on original return as filed. After the Original Return is entered, the user creates adjustments based on the examination. If the User tries to validate the F5344 with incomplete or incorrect information, they are prompted to complete or correct their data:

Upon validation of F5344 a message is displayed and the user can print the form.

5. Is there another source for the data? Explain how that source is or is not used.
No.

6. Generally, how will data be retrieved by the user?
See Item #2 above for data sources. Users retrieve the data from various sources by initiating a data request.

To access the RGS application, users are required to authenticate by providing a username and password. RGS LAN users receive their usernames and passwords after successfully completing the OL5081 form, and receiving approval from their managers. Each LAN username/password is unique and is associated with a group and role within the group. Therefore users' roles and access levels are pre-determined prior the creation of their accounts.

Users access the RGS application either by logging on locally (workstation/laptop) or by mapping to the RGS server to which they have been assigned.

Access to CEAS (Correspondence Examination Automation Support -a separate system) requires the use of an OL5081. After approval of the OL5081, access to CEAS follows the procedures required to log into RGS LAN. The user inputs a SSN number, name control or a tax period and CEAS will return with the case data details in a zip file, or it may return a CFOL data file written in a custom format.

RGS LAN servers will return RTF data in RTF format and the user can have CFOL data on a removable storage device (disk, CD, flash drive). All data stored on a removable storage device is encrypted using GERS. Data destruction follows the procedures set forth in Operation RED.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. After logging in to RGS users may retrieve data by SSN or name.

Access to the Data

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

Based on the need to know, and with approval of RGS management, revenue agents, tax compliance officers, tax examiners, managers, clerks, and system administrators will have access to the system.

Also, RGS uses contractors to develop and maintain the RGS application and to provide engineering services and support. All contractor employees must have properly adjudicated background investigations based on the level of risks associated with their duties. Any contractor who has system administrator duties, or has root access to RGS will have a high risk level background investigation performed prior to assuming the duties.

All work performed by contractor employees is conducted at IRS facilities. All contractor employees will have signed required non-disclosure agreements, and will have had IRS required security training, including UNAX awareness certification.

9. How is access to the data by a user determined and by whom?
RGS utilizes the OL5081 forms for predetermined access and pre-defined roles for LAN users. This allows for the principle of "separation of duties" to be enforced. Each LAN username/password is unique and is associated with a group and role within the group. Therefore users' roles and access levels are pre-determined prior the creation of their accounts.

Contractor access to RGS also uses the OL5081 process. Approval of these is by IRS management or the Contracting Officer's Technical Representative (COTR).

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. If NO, continue to Question 12.
Yes. The following systems, each of which requires an OL5081, share data with RGS: AIMS, Integrated Data Retrieval System (IDRS), and CEAS.

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

- CEAS - Accredited 2/2/07, Expires 2/2/10
- AIMS - Accredited 6/7/06, Expires 6/7/09
- IDRS - Accredited 5/18/06, Expires 5/18/09

12. Will other agencies provide, receive, or share data in any form with this system?
Yes, in accordance with written agreements generally known as Fed/State agreements. Details of Fed/State information exchanges are covered in Implementing Agreements, which normally cover a variety of exchange activities, as well as in Memorandums of Understanding (MOUs), which normally involve specific information exchanges or activities.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
An approved records retention schedule for RGS and associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for RGS inputs, system data, outputs, and system documentation will be published under IRM 1.15.23 *Records Control Schedule for Tax Administration - Examination,* item number to be determined.

14. Will this system use technology in a new way?
No. RGS will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups?
No.

16. Will this system provide the capability to monitor individuals or groups?
No.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. There is a formal appeals process for affected parties. The taxpayer has 30 days to respond to a letter from the IRS stating its position. A formal package, which includes both the IRS and taxpayer positions, is sent to IRS Appeals for a decision. Appeals will review the case file and meet with the affected party prior to the determination.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
Not applicable. RGS is not web-based.

View other PIAs on IRS.gov