Returns Inventory and Classification System – Compliance Decision Analytics (RICS–CDA) Privacy Impact Assessment

PIA Approval Date – Jan. 13, 2010

System Overview:

The Returns Inventory and Classification System – Compliance Decision Analytics (RICS–CDA) application supports the development of a comprehensive set of tools/capabilities that provide decision support, including replacing manual or outdated referrals and claims processing and reporting capabilities and streamlines the case building process. It will further develop a reporting functionality for the Reporting Compliance Case Management System (RCCMS) and an ability to access its compliance data, providing an analytical environment of compliance data. The RICS–CDA application is essential for Tax Exempt/Government Entities (TE/GE) to implement its end–state vision of improving compliance. RICS–CDA provides users access to referrals, claims, and exam information as appropriate. It provides data analytic and reporting capabilities to the employee plans (EP), exempt organizations (EO), Indian tribal government (ITG), federal, state & local governments (FSLG) and tax exempt bonds (TEB) compliance programs.

Systems of Records Notice (SORN):

- IRS 34.037--IRS Audit Trail and Security Records System
- IRS 50.222--Tax Exempt/Government Entities (TE/GE) Case Management Records
- 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:

The system will contain data elements to identify taxpayers and employees. There will be additional data to define the risk compliance level of taxpayers.

A. Taxpayer (available/displayed to user)
   - Social Security Number (SSN)
   - Employer Identification Number (EIN)
   - Taxpayer State
   - Tax period (when the form was filed)
   - Pension Plan Number
     - Taxpayer (only stored in the application)
       - Name
       - Address
       - Phone Numbers
       - Tax Return Information
       - Representative Name
       - Representative Address
       - Return Type
       - Year of Return
       - Document Locator Number (DLN)

B. Employee (available/displayed to user)
   - Name
   - Standard Employer Identifier (SEID)

- Assigned Group Number
- Primary Business Code (PBC)
- Secondary Business Code (SBC)
- Employee Group Code (EGC)
    - Employee (only stored in the application)
        - Address
        - Phone Number
        - Email Address
        - Flexi–Place Location
        - Manager Name
        - Social Security Number
        - Grade and Series
        - Operating Division/Business Unit
        - Employee Group Code
        - Badge Number
        - Employee Role within the RCCMS application

C. Audit Trail Information

- User Identifier/SEID
- Machine Name
- Unique External Key (UEK)
- Events Occurred
- Date and Time of Event
- Outcome of Events

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

A. IRS – RCCMS (TE/GE) Application

- Taxpayer:
    - SSN
    - EIN
    - Taxpayer State
    - Tax period (when the form was filed)
    - Pension Plan Number
    - Name
    - Address
    - Phone Numbers
    - Tax Return Information
    - Representative Name
    - Representative Address
    - Return Type
    - Year of Return
    - DLN
- Employee:
    - Name
    - SEID
    - Assigned Group Number

- PBC
- SBC
- EGC
- Address
- Phone Number
- Email Address
- Flexi–Place Location
- Manager Name
- Social Security Number
- Grade and Series
- Operating Division/Business Unit
- Employee Group Code
- Badge Number
- Employee Role within the RCCMS application

3. Is each data item required for the business purpose of the system? Explain.
Yes. Employee data maintained in the application is necessary to ensure only authorized users have access in and out of the application. In addition, all taxpayer personally identifiable information (PII) is required in the application, as the compliance risk of the taxpayer if analyzed and reported on in RICS–CDA. PII is not transferred to any other application with the exception of audit log information to the Security Audit and Analysis System (SAAS) application for audit review.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Prior to the release of data into the production environment, extensive testing is performed to verify the accuracy, timeliness and completeness of the data elements. Several checks have been implemented within the RICS–CDA application to ensure data input is accurate, complete, and valid. The only data input for the RICS–CDA Information Factory is from the RCCMS application. Data is staged in the RICS–CDA Staging Database prior to being sent to its final location (the Information Factory). The Staging Database ensures data input is valid, accurate, and authentic. The DB checks for invalid values and missing data records from the RCCMS system. Data is transmitted encrypted, via the Enterprise File Transfer Utility (EFTU) transfer protocol to ensure data is not compromised during transfer. In addition, drop down menus are utilized throughout the application to minimize the amount of incorrect or invalid query entries. Data initially provided by the RCCMS application cannot be changed once in the RICS–CDA application. Therefore the application must rely on validity, accuracy, timeliness, and completeness checks available within the RCCMS application.

5. Is there another source for the data? Explain how that source is or is not used.
No. No other source of data is necessary to complete the research purpose of RICS–CDA.

6. Generally, how will data be retrieved by the user?
Users must initially authenticate into the IRS network via the Active Directory. All RICS–CDA users must enter their Windows login credentials a second time in the Business Objects web interface prior to accessing any data within the Information Factory DB. Once in the system, users retrieve data through creating their own selection criteria that is displayed in a report template. These reports can be viewed or printed by authorized application users.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data within the application can be retrieved by SSNs or EINs.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Only authorized IRS employees and a limited number of contractors (application developers who can obtain access to production via approved firecall procedures) with access to the IRS intranet can access the RICS–CDA application. All regular end users, system administrators, and database administrators, have rights to access the application. All permissions are consistent with user designated roles. All access is granted via the Online 5081 (OL5081) process.

> **Role:** System Administrators
> **Permission:** Full access to the application and the Wintel Servers hosting the application.
>
> **Role:** Database Administrators
> **Permission:** Full access to application Structured Query Language (SQL) databases.
>
> **Role:** RICS–CDA Application System Administrators
> **Permission:** Full access to the RICS–CDA application.
>
> **Role:** Power Users
> **Permission:** Access to application and permissions to edit/modify the pre–defined reports.
>
> **Role:** Non–Power Users
> **Permission:** Read–only access to query data in the application's database. User's can edit/modify their own query selection criteria. Non–Power users cannot modify PII data provided by RCCMS.
>
> **Role:** Developers (Computer Science Corporation [CSC] Contractors)
> **Permission:** Read–only access to the production environment upon approved, firecall, emergency procedures.

9. How is access to the data by a user determined and by whom?
Application roles have been identified by RICS–CDA application developers to ensure users only have the level of access needed by the specific user to accomplish his or her job requirements. Potential users must submit a request for access form (OL5081 form) to their local management for approval consideration. Users are not permitted access without a signed OL5081 form from an authorized management official.

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.
Yes.

- Reporting Compliance Case Management System (RCCMS) – RCCMS provides data to RICS–CDA. All PII data that is stored in RICS–CDA was originally sent/provided by the RCCMS application.

- Enterprise Application Integration Broker (EAIB) – The RICS–CDA application interfaces with the EAIB, part of the MITS–18 general support system (GSS) accreditation boundary to perform Negative TIN checking. The EAIB provides RICS–CDA with a list of TINs each RICS–CDA user is not permitted to access.

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

Reporting Compliance Case Management System (RCCMS)

- Certification & Accreditation (C&A) – Approval to Operate (ATO):
  May 25, 2007, expires May 25, 2010 (currently under C&A)
- Privacy Impact Assessment (PIA) – October 26, 2009, expires October 26, 2012

Enterprise Application Integration Broker (EAIB) (part of the MITS–18 GSS boundary)

- Certification & Accreditation (C&A) – Approval to Operate (ATO):
  June 2, 2008, expires June 2, 2011
- Privacy Impact Assessment (PIA) – May 1 2007, expires May 1, 2010

12. Will other agencies provide, receive, or share data in any form with this system?
No. No other systems will provide data to or receive data from the RICS–CDA application.

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 RICS–CDA 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 RICS–CDA inputs and system documentation will be published under Internal Revenue Manual (IRM) 1.15.24, Records Control Schedule for Tax Administration – Tax Exempt and Government Entities (TE/GE), item number to be determined. RICS–CDA data, however, will remain on–line (available to the server) for seven years and then archived off–line (unavailable to the server) as a technical backup.

14. Will this system use technology in a new way?
No. The RICS–CDA application will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. The RICS–CDA application can be used to monitor the status of employee assignments. Within the Referrals Office of TE/GE, the application identifies which Referrals employees have completed the work assigned to them and those who have not. This functionality has been built into the system to ensure RICS–CDA users perform all necessary tasks in a timely matter.

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. The RICS–CDA application can be used to monitor the status of employee assignments within the Referrals Office of TE/GE. The system does not perform actual monitoring of non–compliant taxpayers; however, RICS–CDA provides a thorough analysis of taxpayer non–compliance. Security audit logs are implemented to ensure user activity. Activity concerning PII is fully monitored.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. The RICS–CDA application is only a research/analysis tool and cannot treat taxpayers and IRS employees disparately. It will provide for consistent treatment of all individuals in an equal manner.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not applicable. RICS–CDA does not make any determinations or take any actions towards anyone. The system does not have the ability to confer a negative determination.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No. RICS–CDA is web–based; however, the application is a commercial off the shelf (COTS) solution which has been approved by Enterprise Architecture (EA). For this reason, persistent cookies or other tracking devices are not used to identify web visitors.

View other PIAs on IRS.gov