Embedded Quality Review System – Campus (EQRS–C) – Privacy Impact Assessment

PIA Approval Date – Feb. 1, 2011

<u>**System Overview:**</u>
Embedded Quality Review System – Campus (EQRS–Campus) is used by managers to capture evaluative and non–evaluative data obtained from monitoring taxpayer phone calls and reviewing paper cases and face–to–face contacts. Reports can be generated for planning and training purposes and also for evaluative purposes. Managers use the system to track employee performance and training needs. Another function of EQRS is National Quality Review that is used by independent quality reviewers to capture non–evaluative national and local product review data obtained from monitoring taxpayer phone calls and reviewing paper cases and face–to–face contacts. Reports can be generated for planning and tracking purposes. Management uses the system to track organizational performance against official business performance measures, and to identify opportunities for improvement.

<u>**Systems of Records Notice (SORN):**</u>
- IRS 24.046--Customer Account Data Engine (CADE) Business Master File (BMF)
- IRS 24.030--Customer Account Data Engine(CADE) Individual Master File (IMF)
- IRS 36.003--General Personnel and Payroll Records – Treasury/IRS
- IRS 34.037--IRS Audit Trail and Security Records System
- IRS 26.016--Returns Compliance Programs (RCP)
- IRS 26.019--Taxpayer Delinquent Accounts (TDA)
- IRS 26.020--Taxpayer Delinquency Investigation (TDI) Files

<u>**Data in the System:**</u>

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

A. Taxpayer:
- The Taxpayer Identification Number (TIN)
- Master File Tax code (MFT)
- Tax Period
- IRS Received Date

B. Employee – Data access is limited to employees under the login person's organization only.
- Reviewer Number (limited selection)
- Employee Name (limited selection*)
- Standard Employee Identifier (SEID)
- Organization Code (generated by employee name)
- Input By Number (SEID)

C. Audit Trail Information:
- The application database auditing captures user login as well as data access and modification by employee's SEID
- The web server uses access logs to capture user login, logout and internet protocol (IP) address information.
- EQRS–C has built–in auditing that records Data Collection Instruments (DCIs) accessed by date and employee's SEID

D. Other:
- System–generated unique DCI Number
- Product Line (limited selection)
- Contact Recording
- Contact ID
- Case Type (limited selection),
- Length of Call
- Review Date
- Closing Date
- Organizational Function Program (OFP) Code
- Attribute Codes

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

A. IRS – A weekly extract file from Enterprise Telephone Data (ETD–1) is loaded into the EQRS–C database for call volume data. The data elements include Site Name, Application Number, Volume, and Volume Date.

B. Taxpayer – The Taxpayer Identification Number (TIN), Master File Tax code (MFT), Tax Period, IRS Received Date are collected or recorded from taxpayers during their IRS telephone contact or correspondence.

C. Employee – The Reviewer Number, Employee Number, Employee Name, Input By Number, Product Line, Case Type, Length of Call, Review Date, Closing Date, Organizational Function Program (OFP) Code and Attribute Codes are collected from the employee.

3. Is each data item required for the business purpose of the system? Explain.
Yes. Each item is required to complete the review of actions taken by the tax examiner or customer service representative.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Data is not collected from sources other than IRS records and the taxpayer. The data is considered accurate, timely, and complete.

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

6. Generally, how will data be retrieved by the user?
Data is retrieved by users in a report format from canned or ad hoc reports using begin and end date criteria along with other data filters.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is retrievable by Reviewer Number, Date of Review, Employee Name and Employee SEID. Data is not retrievable by taxpayer TIN. A user cannot download the TIN to a personal computer for spreadsheets. When a user is selecting DCI fields for ad hoc reports, the TIN field is not available as an option to select.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Managers, Quality Staff Employees, Headquarters (HQ) Analysts, Computer System Administrators (CSA), and the Programmers will have access to the data in the system. The users are quality reviewers and/or management officials. With the exception of leads, their employees do not input anything into the system or have access to the system.

A. Role and Permission Levels for EQRS:

- **Role:** Office Assistant/Clerical
- **Permission:** Input/Edit is limited to his or her own organization's (org) assignment plus additional org's and applications assigned. Input cut–off is 45 days from Review Date. Access to View DCI and individual employee reports only, no cumulative employee reports. Org reports are limited to their own org assignment plus additional orgs assigned. Org report access below the Department/Territory level outside user's own org is not allowed. Ad–hoc report access to the employee level outside user's own org is not allowed. Maintenance ability for employee's only. No maintenance abilities for any other user level.

- **Role:** Leads/Technical Leads
- **Permission:** Input/Edit permission is limited to the lead's own org assignment plus additional orgs and applications assigned. Input cut–off is 45 days from Review Date. View DCI and individual employee reports only, no cumulative employee reports. Org reports are limited to own org assignment plus additional orgs assigned. Org report access below the Department/Territory level outside user's own org is not allowed. Ad–hoc report access to the employee level outside user's own org is not allowed. The user level can not create Ad–Hoc Bucket Count Reports. The user level has no maintenance abilities. Must also be able to be monitored as an employee.

- **Role:** Front Line Managers
- **Permission:** Input/edit limited to org assignment plus additional orgs assigned. Input cut–off is 45 days from Review Date. Reports down to individual employee level within own org plus additional orgs assigned. Department/Territory level and above reports nationwide. Maintenance ability for employee's only. No maintenance abilities for any other user level.

- **Role:** Application Managers
- **Permission:** Input/edit limited to org assignment and application plus additional orgs assigned. Input cut–off is 45 days from Review Date. Reports down to individual employee level within own org plus additional orgs and applications assigned. Org report access below the Department/Territory level outside user's own org is not allowed. Maintenance ability for employee's only. No maintenance abilities for any other user level.

- **Role:** Department Managers
- **Permission:** Input/edit for own department plus additional orgs assigned. Input cut–off is 180 days from Review Date. Reports down to individual employee level within own department plus additional orgs assigned. Org report access below the

Department/Territory level outside user's own org is not allowed. Maintenance ability for employee's only. No maintenance abilities for any other user level.

- **Role:** Operation/Territory Managers
- **Permission:** Input/edit for own operation/territory plus additional orgs assigned. Input cut–off is 180 days from Review Date. Reports down to individual employee level within own operation/territory plus additional orgs assigned. Org report access below the Department/Territory level outside user's own org is not allowed. Maintenance ability for employee's only. No maintenance abilities for any other user level.

- **Role:** Planning and Analysis (P&A) Analysts
- **Permission:** No input/edit abilities. Reports down to employee level for own directorship. Org report access below the Department/Territory level outside user's own org is not allowed. No maintenance abilities.

- **Role:** Quality Staff
- **Permission:** No input/edit abilities. Org and ad hoc reports for all levels within directorship down to team. Org report access below the Department/Territory level outside user's own org is not allowed. No maintenance abilities.

- **Role:** Quality Managers
- **Permission:** Input/edit limited to own team plus additional orgs assigned. Input cut–off is 45 days from Review Date. Reports down to employee level for own directorship. Org report access below the Department/Territory level outside user's own org is not allowed. Maintenance ability for employee's only. No maintenance abilities for any other user level.

- **Role:** HQ Personnel
- **Permission:** No input/edit abilities. Org report access below the Department/Territory level outside user's own org is not allowed. No DCI Number or Employee Name on Ad Hoc Reports. No maintenance abilities.

- **Role:** HQ Personnel – employee access needed
- **Permission:** No input/edit abilities. Reports down to employee level for own BOD. Org report access below the Department/Territory level outside user's own org is not allowed. No maintenance abilities.

- **Role:** Site System Coordinator (SSC)
- **Permission:** Input/edit for own directorship. All reports access for all levels of own directorship. Org report access below the Department/Territory level outside user's own org is not allowed. Maintenance abilities for assistors and users in own directorship.

- **Role:** Employee Quality (EQ) Support Team
- **Permission:** Input/edit enterprise wide. All reports for all levels of enterprise. Maintenance abilities for enterprise. Ability to grant Change Site permissions.

- **Role:** On the Job Instructor (OJI)
- **Permission:** Input/edit limited to own org assignment plus additional orgs assigned and Non–Evaluative Other and Non–Evaluative Targeted and Non–Evaluative Test Call review categories. Input cut–off is 45 days from Review Date. View DCI and individual employee reports only for the non–evaluative review types. Cumulative employee

reports on non–evaluative review types only. Org reports limited to own org assignment. Department/Territory level and above reports nationwide. Ad hocs to employee level in own org and Department/Territory level in other orgs. The user level can not create Ad–Hoc Bucket Count Reports. Maintenance ability for employee's only (user level 0). No maintenance abilities for any other user level. Must also be able to be monitored as an employee.

B. Roles and Permission Levels for NQRS

- **Roles:** HQ Personnel/Product Line Analysts
- **Permission:** Input/Edit reviews for designated Specialized Product Review Group (SPRGs) nationwide. Input/Edit cut–off is 90 days after end of reporting period. National and local reports nationwide (all sites, all SPRGs). No maintenance abilities. Input/Edit Volumes for designated SPRGs up to 90 days.

- **Roles:** Centralized National Reviewer
- **Permission:** Input of national (not local) reviews for designated SPRGs for all sites nationwide. Edit ability for own reviews only. Edit cut–off is 7 days after end of reporting period. National (not local) reports nationwide for completed reviews (all sites, all SPRGs). No maintenance abilities.

- **Roles:** Multi site Reviewer
- **Permission:** Input/Edit of national reviews for own directorship for designated SPRGS. Input/Edit of local reviews for own directorship for designated SPRGS. National and local designated SPRGS may differ. Edit cut–off is 7 days after end of reporting period for National review. Input volumes for directorship (designated SPRGs). Volume Input/Edit period begins the day after the end of the reporting period plus 10 days. National reports nationwide for completed reviews (all sites, all SPRGs). Local reports for directorship only. No maintenance abilities.

- **Roles:** Site Reviewer
- **Permission:** Input/edit of national reviews for own site for designated SPRGS. Input/edit of local reviews for own site for designated SPRGS. National and local designated SPRGS may differ. Edit cut–off is 7 days after end of reporting period for National review. Input volumes for site (designated SPRGs). Volume Input/Edit period begins the day after the end of the reporting period plus 10 days. National reports nationwide for completed reviews (all sites, all SPRGs). Local reports for site only. No maintenance abilities.

- **Roles:** Local Reviewer
- **Permission:** Input/edit of local reviews for own site only. Designated SPRGS. National reports nationwide for completed reviews (all sites, all SPRGs). Local reports for own site only. No maintenance abilities.

- **Roles:** Centralized National Reviewer Lead
- **Permission:** Input/edit of only national reviews for all sites nationwide. Designated SPRGS. Input/Edit cut–off is 90 days after end of reporting period. National (not local) reports nationwide (all sites, all SPRGs). No maintenance abilities.

- **Roles:** HQ Data Reader
- **Permission:** No input/edit abilities. National and local reports nationwide for completed reviews (all sites, all SPRGs). No maintenance abilities.

- **Roles:** Data Reader
- **Permission:** No input/edit abilities. National reports nationwide for completed reviews (all sites, all SPRGs). Local reports for own directorship. No maintenance abilities.

- **Roles:** National Quality (NQ) Support Team
- **Permission:** Input/edit enterprise wide. No Input/edit cut–off. National and local reports nationwide (all sites, all SPRGs). Maintenance abilities for enterprise. Input/Edit Volumes.

- **Roles:** Quality Manager
- **Permission:** No input/edit abilities. National and local reports nationwide for completed reviews (all sites, all SPRGs). No maintenance abilities. National Review Management Reports for designated reviewers at the manager's directorship sites.

9. How is access to the data by a user determined and by whom?

Access to the data is determined by the manager based on a user's position and need–to–know. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules in Online Form 5081, Information System User Registration/Change Request. The user's access is restricted. Managers do not have the ability to view data on employees who are not under their supervision. Also, a user's access to data is based on (and limited by) the permission level granted to the user. The application has been developed and is maintained by IRS employees.

Note: Contractors do not have access to the application.

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. A weekly extract file from Enterprise Telephone Data (ETD–1) is loaded into the EQRS–C database for call volume data. The data elements include Site Name, Application Number, Volume, and Volume Date. Call volume data from ETD–1 is used in EQRS–C to calculate weighted performance measures for various IRS product lines.

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

Yes. ETD–1 is a non–FISMA, non–certifiable application. Therefore, it does not have an approved Security Certification and Privacy Impact Assessment.

Enterprise Telephone Data (ETD–1)
- Certification & Accreditation (C&A) – April 13, 2006
- Privacy Impact Assessment (PIA) – April 26, 2006

12. Will other agencies provide, receive, or share data in any form with this system?

No other agencies will share data or have access to the data in this system other than the Treasury Inspector General for Tax Administration (TIGTA) and the Government Accountability Office (GAO) as part of their official oversight responsibilities.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
EQRS–C recordkeeping data is approved for destruction three years after close of reporting year for managerial review and six years after close of reporting year for product review under NARA Job No. N1–58–06–8, item 1, and published under 1.15.31 Records Control Schedule for Customer Service, item 10(2). However, in reviewing current EQRS–C recordkeeping practices for completion of this PIA, system owners and the IRS Records Office determined that a re–evaluation of that approved 2006 retention is in order. W&I and the Records Office will work together to validate and potentially update EQRS–C dispositions to better fit current data collection activities and maintenance needs. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6.

14. Will this system use technology in a new way?
No. EQRS–C 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 system provides the capability to identify, locate, and monitor/review employees for training and evaluative purposes only.

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 system provides the capability to identify, locate, or monitor individual employees or groups of employees. Reports are generated by Organization Code for training purposes. Access to the EQRS–C is controlled by Application Support personnel. The manager will request a user be added. They must fill out Form 5081, Information System User registration/Change Request, to request access to the System. The Application Support personnel determine to which group and menu the user will have access. Unauthorized Access (UNAX) training is also provided to inform users of the statutory rules governing and the IRS' policy on unauthorized access and inspection of records by IRS employees.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. EQRS–C is designed to facilitate a required manual process. There is no disparate treatment of individuals or groups. Product review is selected using an algorithm for random selection.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. All data comes from managerial or product reviews of employee work. The manager visually inspects any defects cited. The employee has the opportunity to explain, refute, or otherwise respond to the data via a Dispute Resolution Panel. The system also has an option to remove the data and exclude it from employee performance.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No. The system does not use persistent cookies or other tracking devices to identify web visitors.

View other PIAs on IRS.gov