

Date of Approval: March 16, 2016

PIA ID Number: **1664**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Embedded Quality Review System - Field, EQRS-F

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Embedded Quality Review System-Field (EQRS-F) ID#368

Next, enter the **date** of the most recent PIA. 3/7/2013

Indicate which of the following changes occurred to require this update (check all that apply).

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>Yes</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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 Embedded Quality program provides a tool for managers and quality reviewers to assess performance via the Embedded Quality Review System-Field (EQRS-F). EQRS-F is comprised of two main modules: NQRS (National Quality Review System) for non-evaluative organizational reviews and Embedded Quality Review System (EQRS) for evaluative/non-evaluative managerial performance reviews. The database contains information from evaluative reviews conducted by managers and organizational quality reviews conducted by the national review staff. EQRS-F integrates data from the Integrated Collection System (ICS), the Automated Insolvency System, and the Examination Returns Control System (ERCS). The ICS/AIS/ERCS extracts reduce the burden for Field Compliance managers and the National Quality Review staff by eliminating the need for managers and reviewers to input data elements currently available on ICS/AIS/ERCS when performing reviews. The EQRS-F application contains privacy information in the form of Taxpayer Identification Numbers (TINs), taxpayer names and employee performance data.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No Practitioner Tax Identification Number (PTIN)

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

A mitigation strategy is currently not required. SSNs are needed to track individual case reviews.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	No	No
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No

No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

<u>No</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

TIN/SSNs are needed to track the individual case reviews conducted by the managers and quality review staff. Access to TIN/SSN data is limited based on the user's position in the organization and on a need to know basis. Managers can retrieve TIN/SSN data for their employee's taxpayer cases within their chain of command. Access to TIN/SSN data by quality review staff is limited to users based on a need to know. Quality review staff are conducting reviews of the actions taken by Collection, Examination, Specialty and BSA employees on taxpayer cases.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

The TIN/SSN data used in the EQRS-F system is not used to make a determination about an individual's rights, benefits and privileges. EQRS-F is used to conduct manager reviews of employee cases and quality reviews of cases. For most of the functions, the TIN/SSN and Taxpayer name is uploaded into EQRS-F with a weekly extract file from the ICS, AIS and ERCS. This ensures the accuracy of the data.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

<u>SORNS Number</u>	<u>SORNS Name</u>
00.008	Recorded Quality Review Records
24.030	CADE Individual Master File
24.046	CADE Business Master File (BMF)
24.009	Lien Files
26.019	Taxpayer Delinquent Account (TDA) Files
26.020	Taxpayer Delinquency Investigation (TDI) Files
36.003	General Personnel and Payroll Records
42.021	Compliance Programs and Project Files

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. *Redacted Information For Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Integrated Collection System (ICS)	Yes	09/19/2013	Yes	03/16/2015
Automated Insolvency System (AIS)	Yes	04/21/2014	Yes	10/02/2015
Examination Returns Control Selection (ERCS)	Yes	01/29/2014	Yes	02/19/2015

11b. Does the system receive SBU/PII from other federal agency or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No
14. Does this system use privacy-sensitive technologies such as mobile, cloud, global position system (GPS), biometrics, RFID, etc.? No
15. Does the system use cloud computing? No
16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

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

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? PII data in the EQRS-F application is not used for legal or administrative action with a taxpayer. Notice, consent, and due process are provided via ICS, AIS, ERCS, and its related tax forms and instructions.

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

PII data in the EQRS-F application is not used for legal or administrative action with a taxpayer. It is just used to evaluate case quality by the manager and for national review purposes. Due process will not apply to this application for taxpayers. Due process for employees will follow the normal performance management process outlined in the IRM and National Agreement. The system ensures "due process" by allowing affected parties (IRS employees) to respond to any negative determination, prior to final action. All EQRS-F data comes from managerial reviews of employees' work. The employee has the opportunity to explain, refute, or otherwise respond to the data via the Dispute Resolution process (part of the 2009 National Agreement and IRM 6.771.1). The system also has an option to remove the data and exclude it from an employee's performance report.

I. INFORMATION PROTECTION

20. 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 Operated

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

IRS Employees? Yes

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level(Read Only/Read Write/Administrator)</u>
Users	Yes	Read and Write

Managers	Yes	Read and Write
Sys. Administrators	No	
Developers	Yes	Read-Only

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? User access to data is limited based on their position in the organization and the need-to-know. The application restricts access to PII data based on the user's permission level and organization. Managers are only able to access PII data within their chain of command. User access is requested through the Online 5081 (OL5081) process. The level of access granted to users is consistent with the OL5081 form and only privileges that are required for the user to perform the job functions are granted. As part of the annual recertification of the OL5081 process, managers are required to validate that their employees still need access to the system. The System Coordinator serves as gatekeepers by verifying each user access request, as well as verifying that the level of access is in compliance with their role.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ?
Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22a. 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.

EQRS and NQRS recordkeeping data is approved for destruction under newly approved Job No. N1-58-12-16 (signed 11/27/12). This 2012 disposition approval by NARA supersedes 2006 disposition determinations approved under Job No. N1-58-06-8. EQRS data is approved for destruction 3 years after close of reporting year. This is published in IRS Document 12990, Records Control Schedule 31 for Customer Service, item 10(2). NQRS data is approved for destruction 6 years after close of reporting year. This is published in IRS Document 12990, Records Control Schedule 21 for Strategic Planning, item 17. 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 Managing Electronic Records. The method used for sanitization will follow NIST SP 800-88 guidelines.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 4/24/2015

23.1 Describe in detail the system s audit trail. The EQRS-F application had an ESAT approved audit plan April 8, 2012. The audit plan was recently updated and a UWR was submitted for ESAT to revalidate before implementing. The EQRS-F application creates an audit log record when a user logs on, logs off, changes password, assigns a user permission level, modifies a user record, assigns proxy access, creates, deletes or modifies review DCI data, etc. The EQRS-F application produces audit records that contain sufficient information to determine what type of even occurred, when and where the event occurred, the source of the event, the outcome of the event, and the identity of any user/subject associated with the event.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Rational ClearQuest stores the test specifications used to test and validate each defect, and the System Test Plan is completed and approved before any release to production.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? System testing occurs against the current requirements throughout the development life cycle before each release. Testing includes Unit, Regression, Acceptance, Accessibility, and Integration testing. Privacy concerns are addressed in developer's meeting when discussing new defects that are identified. Annual Security Controls Assessment (ASCA) testing occurs during annual security testing.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees:	<u>Under 50,000</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>100,000 to 1,000,000</u>
26d. Other:	<u>No</u>

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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? No

End of Report
