Date of Approval: 10/13/2017 PIA ID Number: **2877**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Automated Questionable Credits, AQC

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.

Automated Questionable Credits, AQC #1015

Next, enter the **date** of the most recent PIA. 10/8/2014

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

No ___ Addition of PII
No ___ Conversions
No ___ Anonymous to Non-Anonymous
No ___ Significant System Management Changes
No ___ Significant Merging with Another System
No ___ New Access by IRS employees or Members of the Public
No ___ Addition of Commercial Data / Sources
No ___ New Interagency Use
No ___ 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)

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

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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 Automated Questionable Credits (AQC) Program is part of the Return Integrity & Correspondence Services (RICS) under the purview of the Director of the Refund Integrity Correspondence, Wage and Investment (W&I). The AQC application is designed to protect revenue by covering cases that are currently untreated or undertreated by other available programs across the IRS. AQC is a program that the IRS introduced to protect significant additional revenue at a relatively low cost and response rate. For cases to be considered for treatment by AQC, they must meet the appropriate AQC criteria. RICS work is part of an overall revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. Due process is provided pursuant to 26 United States Code (USC).

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)
No	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).

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The AQC database requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	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
Yes	Tax Account Information	Yes	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

Selected	SBU Name	SBU Description
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.
Yes	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)

Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes SSN for tax returns and return information is Internal Revenue Code Section 6109
No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No PII for personnel administration is 5 USC
No PII about individuals for Bank Secrecy Act compliance 31 USC
No 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.

RICS work is part of an overall IRS revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. The AQC database is primarily utilized by employees of RICS for cases that are currently untreated or undertreated by other available programs across the IRS. AQC is a program that the IRS introduced to protect significant additional revenue at a relatively low cost and response rate. Collection of PII is necessary to research and resolve these 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 PII maintained in the AQC database is provided directly from existing IRS systems and approved programs. Input of the data received is both systematically and manually entered into the AQC database. Assignment of AQC to tax examiners is manually entered by managers/administrators. Accuracy and completeness of data is inherited from the existing IRS systems.

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.

SORNS Number	SORNS Name
Treasury/IRS 34.037	Audit Trail and Security Record System
Treasury/IRS 42.021	Compliance Programs and Projects 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. ##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.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Electronic Fraud Detection System (EFDS)	Yes	01/16/2015	Yes	06/23/2017
Business Objects (BOE)	No		No	06/23/2017

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

11c. Does the system receive SBU/PII from State or local agency(s)? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
1040	US Individual Income Tax Return
14039	Identity Theft Affidavit

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? 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, 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?
Notice and consent are provided in the tax forms and instructions pursuant to 5 USC.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
Notice, consent and due process are provided in the tax forms and instructions pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read and Write

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? A potential user will request access via the Online 5081 (OL 5081) system. This request has to be approved by the potential user's manager based upon a user's position and need-to-know. If approved, the request is then forwarded to the administrators of the system for the creation of a new user identification and password.

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? Yes

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? No

22b. 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.

The AQC database is unscheduled. W&I will work with the IRS Records Office to draft a request for records disposition authority for approval by the National Archives and Records Administration. When approved, disposition instructions for AQC inputs, outputs, master files data, and system documentation will be published in Records Control Schedule (RCS) Document 12990, likely under RCS 29 for Tax Administration - Wage and Investment. AQC is a W&I tracking database of untreated and/or undertreated cases from EFDS for tax examiner research which is currently not covered under other IRS programs. W&I proposes AQC data disposition instructions to destroy 3 years after case is closed. The data in the AQC database will be backed up daily and weekly for purposes of restoration.

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)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the systems audit trail. The audit trail contains the audit trail elements as required in current Internal Revenue Manual 10.8.1, Audit Logging Security Standards.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. The system follows Federal Information Processing Standard Publication 200 minimum security requirements for the appropriate security controls and requirements as described in National Institute of Standards and Technology Special Publication 800-53 Revision 3. The appropriate policy checkers, network checkers, security scans, and critical updates are maintained. The technical controls that the reporting database has in place are mainly inherited from the General Semantics (GS). The system administrator role includes: 1) Controlling remote access to the system; 2) Installing Operating System updates and patches; 3) Running system policy checker; 4) Ensuring the system configuration remains in compliance with the Standard Query Language (SQL) server policy checker. The database administrator role includes: 1)

Adding/Removing users to/from SQL server; 2) Assigning access levels to SQL server users; 3) Creating and maintaining database instances; 4) Running the SQL Server policy checker; 5) Ensuring the SQL Server configuration remains in compliance with the SQL server policy checker; 6) Backing up the data. All other administrative and technical controls are inherited by the GS. All RICS applications will be using databases housed on a SQL server using Windows authentication only. SQL Server authentication will be disabled on the SQL server to comply with IRM requirements. Database roles will be created for each database, and proper "least privilege" permissions will be assigned on all pertinent database objects (tables, stored procedures, views, etc.) to these roles. Rather than adding each application user as a login to the SQL server, we will create local Windows groups on the SQL server with appropriate names describing the application and access level within in the name (ie, Contacts_Admin and Contacts_StdUser). These local Windows groups will then be added as SQL logins and given only the permission to the database needed for the application. In addition, the local Windows groups will then be placed in the corresponding database role. The security administrator, based upon the OL 5081, will place the IRS user into the appropriate local Windows groups, which has already been mapped to the appropriate access level on the SQL server.

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:	Under 50,000
26b. Contractors:	Not Applicable
26c. Members of the Public:	100,000 to 1,000,000
26d. Other:	Yes

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