Date of Approval: **October 27, 2020**

PIA ID Number: **5562**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Automated Questionable Credits, AQC

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

AQC, PIA #2877

What is the approval date of the most recent PCLIA?

10/13/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Wage and Investment Division Risk Committee (W&I RC)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

No

GENERAL BUSINESS PURPOSE

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 Compliance, 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).

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Delivery of governmental benefits, privileges, and services

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

SSNs are necessary to distinguish legitimate from non-legitimate refunds filed - especially when there is no other means available for that business requirement.

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.

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Standard Employee Identifier (SEID)

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

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.

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

Are there other types of SBU/PII used in the system?

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 42.021 Compliance Programs and Projects Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Electronic Fraud Detection System (EFDS)
Current PCLIA: Yes
Approval Date: 1/10/2018
SA&A: Yes
ATO/IATO Date: 6/23/2017

System Name: Business Objects (BOE)
Current PCLIA: No
SA&A: No

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1040 Form Name: U.S. Individual Income Tax Form

Form Number: 14039 Form Name: Identity Theft Affidavit

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

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

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Notice and consent are provided in the tax forms and instructions pursuant to 5 USC.

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

No

Why not?

Notice, consent and due process are provided in the tax forms and instructions pursuant to 5 USC. The IRS has the legal right to ask for information per Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for".

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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

RCS 32 Item 37-Electronic Filing - Questionable Refund Project (ELF-QRP). ELF-QRF analyzes electronically filed tax returns to determine if a return should be further reviewed by local Questionable Refund Detection Teams (QRDT). The database contains extract, selection and characteristic criteria for identifying potentially fraudulent individual tax returns. RCS 32 Item 38-Questionable Refund Project (QRP). QRP analyzes, categorizes, codes and scores data on returns to identify potentially fraudulent income tax returns. The database contains taxpayer data and selection criteria identified by the Questionable Refund Detection Team. AUTHORIZED DISPOSITION Delete when 1 year old or when no longer needed for administrative, legal, audit or other operational purposes, whichever is sooner. A. Inputs: These records include, but are not limited to, electronically filed tax return data and QRP adjusted return selection parameters. AUTHORIZED DISPOSITION Delete electronic media when the information is obsolete, superseded or no longer needed in current operations. Destroy paper when 1 year old or when no longer needed for administrative, legal, audit or other operational purposes, whichever is sooner. See the QRP Computer Programmers Handbook and the Computer Operator's Handbook. RCS 29 Item 55-58. All records housed in the Wage and Investment system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedule (RCS) 29 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

The audit trail contains the audit trail elements as required in current Internal Revenue Manual 10.8.1, Audit Logging Security Standards. In particular, RICS systems keep records of the following: # 10.8.1.4.3.2 (05-09-2019) AU-3 Content of Audit Records (1) IRS information systems shall generate audit records containing information that establishes: (AU-3) (L, M, H) a.What type of event occurred. b.When the event occurred. c.Where the event occurred. d.The source of the event. e.The outcome of the event. f.The identity of any individuals or subjects associated with the event.

PRIVACY TESTING

Does the system require a System Test Plan?

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 5. 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.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: 100,000 to 1,000,000

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

All records for revenue protection

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

Yes

Does your matching meet the Privacy Act definition of a matching program?

Yes

Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Yes

ACCOUNTING OF DISCLOSURES

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