Date of Approval: **January 22, 2020**

PIA ID Number: **4624**

## SYSTEM DESCRIPTION

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

Automated Quarterly Excise Tax Listing, AQETL

*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?*

Automated Quarterly Excise Tax Listing, AQETL 566

*What is the approval date of the most recent PCLIA?*

12/28/2016

*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.*

Financial Services Governance Board FSGB

*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?*

Yes

## 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.*

Automated Quarterly Excise Tax Listing (AQETL) is an internal web-based application used by the Internal Revenue Service to monitor Excise Taxes filed on Internal Revenue Service (IRS) Form 720. AQETL is used by the Office of the Chief Financial Officer (CFO) Headquarters staff and the Ogden Campus employees to identify and resolve anomalies in the information provided in excise tax filings. The Excise Tax Return lists many different types of taxes (IRS numbers/abstracts) (e.g. there are taxes on many different types of fuels (gasoline, diesel, gasohol, aviation, etc.). The purpose for reviewing tax returns data is to ensure the proper amounts are transferred (certified) to the correct Trust Funds. The application compares the current returns data to the prior returns data, and alerts CFO Headquarters (Washington DC) and Ogden Campus Exam/AUR employees to possible tax anomalies (errors).

## 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

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

There is no reasonable alternative means for meeting business requirements.

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

The AQETL system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax return.

Employer 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

Mailing address

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.

*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.*

EIN and TIN information are needed to collect and process Excise Tax information.

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

Data has been verified at the source (i.e., the IRS Business Master File (BMF)) and AQETL checks the File ID to make sure it has been received. The original data from the IRS BMF is not verified again once it is in AQETL; the only verification is whether data is extracted and put into AQETL.

## 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 42.021 Compliance Programs and Projects Files

IRS 24.046 Customer Account Data Engine Business Master file

## 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: BMF Master File
Current PCLIA: Yes
Approval Date: 8/27/2018
SA&A: Yes
ATO/IATO Date: 2/25/2019

*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: Form 720 Form Name: Quarterly Federal Excise Tax Return

*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?*

Information is provided through IRS Knowledge and Privacy instructions on Form 720.

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

No

*Why not?*

We ask for the information on form 720 in order to carry out the Internal Revenue laws of the United States. We need it to figure and collect the right amount of tax. Miscellaneous excise taxes are imposed under Subtitle D of the Internal Revenue Code.

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

Through the normal Tax process pursuant to title 26 of the United States Code.

## 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 Only

Managers: Administrator

System Administrators: Administrator

Developers: Read Write

*How is access to SBU/PII determined and by whom?*

The Service Center User, CFO User, Application Administrator, Developer, System Administrator, Web Server Administrator, and Database Administrator will have access to the AQETL system. The following table details the AQETL roles and privileges. All users of AQETL are IRS employees. Users Permissions: Service Center User: The Service Center User accesses the application via a web interface and has access to all trust funds data (IRS numbers/abstracts) to review error transactions that occur within the EIN range associated with each employee. This user also has access to the Verify Module which allows the user to post comments, and verify the data that displays abstract number, tax period, cycle, current period dollars, and current period error numbers, and view un-posted transactions. CFO User: The CFO User accesses the application via a web interface and has access to the records by Trust Fund and Abstract number. This user also has access (1) to the Verify Module, (2) to the AQETL reports; and (3) has the ability to mark errors as corrected. Application Administrator: The Application Administrator has all of the permissions of the CFO User plus additional privileges via the Admin Module. The Application Administrator accesses the application via a web interface and has the privileges to: (1) add, delete and modify user information; (2) add, delete and modify trust fund definitions, sub trust account names and abbreviations, sub-trust abstract numbers, print order and owners; (3) add, delete and modify period dates and posting cycles; (4) add, delete and modify Service Center information; (5) add, delete and modify Service Center names, numbers and contact information; (6) unlock user accounts, and 7) view the application audit logs. Developer: The Developer manages the application functionality and modifies the application code. Database Administrator (DBA): The DBA manages all database functionality and makes configuration updates to the Structured Query Language (SQL) Server database. Web Server Administrator: The Web Server Administrator manages all web server functionality and makes configuration updates to the Internet Information Services web server. Systems Administrator (SA): The SA has full Operating System (OS) level administrative control over the Windows servers and is responsible for applying security patches/updates to the OS. The System Administrator also runs Law Enforcement Manual (LEM) checkers against the Windows servers.

## 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.*

AQETL data is approved for destruction when one year old or when no longer needed for administrative, legal, audit, or other operational purposes (in accordance with Job No. N1-58-97-13, item 12/A and published in IRM 1.15.35). DAA-0058-2017-0002 RCS 32, item 12 Disposition: Temporary. Delete/Destroy when 7 years old.

## SA&A OR ASCA

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

Yes

*What date was it completed?*

4/25/2018

*Describe the system's audit trail.*

The Audit Plan for AQETL has become the property of the Enterprise Security Audit Trail (ESAT) Office. The ESAT office provides a security auditing tool that allows collection retention and review of Enterprise Security audit events.

## PRIVACY TESTING

*Does the system require a System Test Plan?*

Yes

*Is the test plan completed?*

Yes

*Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?*

DocIT Repository - testing is performed in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy.

*Were all the Privacy Requirements successfully tested?*

Yes

*Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?*

No

*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?*

Data has been verified at the source (i.e., the IRS BMF) and AQETL checks the File ID to make sure it has been received. The original data from the IRS BMF is not verified again.

## 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: Under 5,000

Members of the Public: Under 100,000

Other: No

## 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?*

Yes

*Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.*

Monitoring of IRS employee use of the system is performed to prevent against unauthorized access.

*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