Date of Approval: December 28, 2016 PIA ID Number: **1857**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Automated Quarterly Excise Tax Listing, AQETL

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 Quarterly Excise Tax Listing, AQETL 566

Next, enter the **date** of the most recent PIA. 11/7/2013

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? 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.

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 Cincinnati Service Center 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 Cincinnati Service Center employees to possible tax anomalies (errors).

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)**
No	**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 AQETL system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer.

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**
Yes	**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**
No	**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.

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

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

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.

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
Treas/IRS 42.021	Special 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. ## 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
BMF Masterfile	Yes	04/24/2015	Yes	02/25/2016

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 (-ies)? 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
Form 720	Quarterly Federal Excise Tax Return

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

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? 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.

19. 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.

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-Only**
Managers	**Yes**	**Administrator**
Sys. Administrators	**Yes**	**Administrator**
Developers	**Yes**	**Read And Write**

Contractor Employees? No

21a. 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 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.

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? 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.

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 and published in IRM 1.15.35). The Business Unit and the Records Office agree this disposition requires future review. A more concrete retention may be preferred. I am proposing to keep these records a minimum of seven years until a proper records schedule can be created.

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? 11/10/2016

23.1 Describe in detail 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.

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?
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 once it is in AQETL; the only verification is whether data is extracted and put into AQETL.

24b.1. If **completed**, 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.

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? Yes

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?
Yes

If **yes,** provide the date the permission was granted. 9/30/2016

25b. **If yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy? Yes

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: Under 5,000
26c. Members of the Public: Under 100,000
26d. Other: No

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? Yes

If **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.

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