Automated Quarterly Excise Tax Listing (AQETL) –
Privacy Impact Assessment (PIA)

PIA Approval Date: October 4, 2010

System Overview

AQETL is an internal web-based application used by the Internal Revenue Service (IRS) to monitor Excise Taxes filed on IRS Form 720. AQETL is used by the Office of the Chief Financial Officer (CFO) Headquarters and staff and 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).

Systems of Records Notice (SORN):

- Treasury/IRS 24.046 - CADE Business Master File
- Treasury/IRS 34.037 - Audit Trail Lead Analysis System
- Treasury/IRS 42.002 - Excise Compliance Programs

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer:
- Employer Identification Number (EIN)
- Employer Name (First 20 Characters)

B. Employee:
- Username and password for IRS Users to log into the system.

C. Audit Trail Information: The system collects the following audit trails data items:
- Date and time that the event occurred;
- The unique identifier (e.g., user name) of the user or application initiating the event;
- Type of event;
- Subject of the event (e.g., the user, file, or other resource affected) and the action taken on that subject; and
- The outcome status (success or failure) of the event. Furthermore, systems that store or process taxpayer information includes the following data elements, where applicable:
    - The type of event (e.g., command code)
    - The terminal and employee identification
    - Date and time of input.

D. Other: AQETL does not contain data other than taxpayer or employee data.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS: Business Master File (BMF): The data elements from IRS Form 720 ("Quarterly Federal Excise Tax Return") are transmitted electronically from the BMF system to the AQETL system via two data extract files (B11 and B12) using the 701 Extract Process. The data elements are transmitted on a weekly basis using EFTU.

B. Taxpayer: Taxpayer information is provided via the IRS Form 720 "Quarterly Federal Excise Tax Return" that the taxpayer completes.

C. Employee: AQETL contains the name, user ID and password.

3. Is each data item required for the business purpose of the system? Explain.
Yes, each data item is required for the business purpose of the system. 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 to the prior returns, and alerts CFO Headquarters (Washington DC) and Cincinnati employees to possible tax anomalies (errors).

4. How will each data item be verified for accuracy, timeliness, and completeness?
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.

AQETL has field level checks for the following input text fields of the web interface:

- Input Field: Password
- Requirement: IRS requirements for minimum character length and complexity.

- Input Field: EIN Search Field
- Requirement: Digits or hyphens, unlimited characters.

- Input Field: Name Search
- Requirement: No restrictions on input. Accepts characters and digits of any length.

The input validations limit passwords to the IRS requirements for minimum character length and complexity and EINs to nine digits. The application also enforces input for these required fields.

Data checks and validations are made against the B11, B12, and PRN files. The B11 and B12 files are validated by SQL Server through the use of constraints by checking the incoming B11 and B12 files extract cycle date to determine if the data was previously loaded. If the data was not previously loaded, the database checks the character length of the files. After the length is validated, a stored procedure is triggered to format the data for the DB. The PRN files are validated by checking the files for valid revenue amounts (i.e., a number greater than 0) and checking that there are eight files. If either of these validations fails, the data will be viewed as invalid and will not be loaded into the database.

5. Is there another source for the data? Explain how that source is or is not used.
No, there is no other source for the data.

6. Generally, how will data be retrieved by the user?
The data is generally retrieved via four (4) modules. These modules include: (1) Verify; (2) Reports; (3) Look Up; and (4) Administrative (limited to certain users).

Users can query for specific taxpayer records by EIN or Name, which can help Users distinguish the type of tax being monitored.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, data can be retrieved by EIN and name.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

The Service Center User, CFO User, Application Administrator, Developer, System Administrator, Web Server Administrator, and Database Administrator will have access to the AQETL system.

Listed below are the AQETL roles and privileges. All users of AQETL are IRS employees.

- **Users:** Service Center User
- **Permissions:** 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.

- **Users:** CFO User
- **Permissions:** 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.

- **Users:** Application Administrator
- **Permissions:** 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.

- **Users:** Developer
- **Permissions:** The Developer manages the application functionality and modifies the application code.

- **Users:** Database Administrator (DBA)
- **Permissions:** The DBA manages all database functionality and makes configuration updates to the SQL Server database.

- **Users:** Web Server Administrator
- **Permissions:** The Web Server Administrator manages all web server functionality and makes configuration updates to the Internet Information Services web server.

- **Users:** Systems Administrator (SA)
- **Permissions:** The SA has full Operating System 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.

No contractor has access to the AQETL system.

9. How is access to the data by a user determined and by whom?
Access to AQETL data is based on roles assigned to the system user. Three (3) user roles exist each having their own assigned access privileges to functions and data within the application. The three user roles are: (1) Service Center User; (2) CFO User, and (3) Application Administrator.

The ability to input information in AQETL is based on access privileges and restrictions built into the client application. The access to these privileges is managed through the use of Online 5081 (OL5081). Only authorized users with appropriate privileges can input information to AQETL.

After the employee's manager has approved the request in the OL5081 system, the Application Administrator is informed of the pending request via email. The Application Administrator verifies that the request is valid and creates the user using a unique username and password. The user will receive an email from the OL5081 system when the Application Administrator has added the user to the AQETL user database. The Application Administrator then forwards the new user their username and password via secure email.

When a User has been approved for access to the application by his/her manager, the OL5081 system sends an email to the User, providing an approval notification. The User then logs into the OL5081 system, reads the Rules of Behavior, and provides an "electronic signature," acknowledging that he/she has read, understands, and agrees to abide by the Rules of Behavior within 45 days or else the account is removed from the database. Further, if the user account is inactive for 45 days the account is removed from the database.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
The data elements from IRS Form 720 ("Quarterly Federal Excise Tax Return") are transmitted electronically from BMF to AQETL via two data extract files (B11 and B12) using the 701 Extract Process. The data elements are transmitted on a weekly basis using EFTU.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes.

- **Application Name:** BMF
- **Certification and Accreditation (C&A) Authority to Operate (ATO) Date:** 06/14/2010
- **Privacy Impact Assessment (PIA) Date:** 03/16/2010

12. Will other agencies provide, receive, or share data in any form with this system?
No other agencies will provide, receive, or share data in any form with this system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
All printed output is handled and secured in accordance with the IRS sensitive output handling organizational policy. AQETL-related records are scheduled under IRM 1.15.32, Item 12 (NARA Job No. N1-58-97-13, approved 2/9/98). System data is approved for destruction when 1 year old or when no longer needed for administrative, legal, audit or other operational purposes, whichever is sooner.

AQETL audit trail archival logs are retained for 6 years, unless otherwise specified by a formal Records Retention Schedule developed in accordance with IRM 1.15, Records Management. All printed output is handled and secured in accordance with the IRS sensitive output handling organizational policy.

14. Will this system use technology in a new way?
No, the system will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No, the system is not used to identify or locate individuals or groups.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No, this system does not provide the capability to monitor individuals or groups. IRS Users can only view and verify if the data is in the right tax field.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.
No, AQETL does not have the ability to allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
AQETL does not impact due process rights of taxpayers/employees.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
No. There are no transactions taking place within the application and, therefore, no cookies will be used in this application.

View other PIAs on IRS.gov