Automated Quarterly Excise Tax Listing Milestone 4B (AQETL) – Privacy Impact Assessment

PIA Approval Date – Nov. 26, 2007

Targeted deployment date – March 2008

Purpose of the System

AQETL is an internal Web-based application used by the Internal Revenue Service to monitor Excise Taxes filed on IRS Form 720. AQETL is used by the Office of the Chief Financial Officer and Cincinnati 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). For example, 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 employees to possible tax anomalies (errors).

Systems of Records Notice (SORN)

- Treasury/IRS 42.002 - Excise Compliance Programs
- Treasury/IRS 34.037 - Audit Trail Lead Analysis System

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

At a minimum, IRS systems are required to record to the following data elements:
- 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

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

A. IRS:
AQETL is a Web-based application used by the Internal Revenue Service to monitor Excise Tax returns data filed on IRS Form 720 ("Quarterly Federal Excise Tax Return"). The data elements from the form are transmitted from the IRS Business Master File (BMF) by two data extract files (B11 and B12) using the 701 Extract Process and is transmitted electronically every month using the Enterprise File Transfer Utility (EFTU). This process will be done on a weekly basis once the application is fully deployed in March 2008. In addition, eight PRN files are transmitted from the IRS BMF and are loaded into the AQETL database at the beginning of the quarter using the Enterprise File Transfer Utility (EFTU).

In addition, AQETL development and production servers rely on the Modernization Information Technology Services (MITS)-30 Wintel Application Servers General Support Systems (GSSs). AQETL also relies on the following MITS GSSs for infrastructure support:

- MITS-1 IRS Perimeter Security
- MITS-17 Enterprise Systems Domain
- MITS-26 Enterprise Remote Access (ERAP)
- MITS-30 Wintel Application Servers
- MITS-32 IRS Workstations and Support
- MITS-34 Enterprise Network

B. Taxpayer:
Taxpayers provide the data elements when filing the IRS Form 720 ("Quarterly Federal Excise Tax Return").

C. Employee:
IRS employees are the only users in AQETL. The following three types of Users are the only ones that have the ability to provide comments/notes within AQETL:

- Service Center User
- CFO User
- Application Administrator

CFO employees cannot make changes to the data on the IRS BMF.

D. Other Federal Agencies: None.

E. State and Local Agencies: None.

F. Other third party sources: None.

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 (FEXC01 GYYYYNN.PRN through FEXC08 GYYYYNN.PRN). If either of these validations fail 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?
Once Users are verified, they can access the application on the IRS Intranet and have four Modules where they can access the data. 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 following users configure, operate, and maintain AQETL. 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: 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) unlocks user accounts, 7) and view the application audit logs.

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:
Developer
Permissions:
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.

Users:
Web Server Administrator
Permissions:
The Web Server Administrator manages all Web server functionality and makes configuration updates to the IIS Web server.

Users:
Systems Administrator (SA)
Permissions:
The SA has full 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.

Lockheed Martin is the only contractor currently working on the application and are the application developers. The contractors will not be retained after the application has been deployed in March 2008.

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 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.

Lockheed Martin, the sole contractor on this application, has staff-like access and is required to undergo a Security Screening Investigation (SSI) unless a Task Order specifies elsewhere that another type of investigation is more suitable to the circumstances. Any Contractor employee who is required to have an investigation is not permitted to work on the contract without the required investigation. Access to IRS facilities, information systems, security items and products, and sensitive but unclassified information may be denied or revoked based upon unsanctioned, negligent or willful action on the part of the Contractor or the Contractor's employees.

Prior to beginning any work under a task order, all identified Contractor employee(s) will undergo a security screening (which ranges from minimal checks to a full Background Investigation). Upon favorable completion of the interim security screening, Personnel Security will grant the Contractor employee(s) interim staff-like access to IRS facilities, systems, information and/or data, as applicable to task order performance. Investigations which reveal derogatory information about a Contractor employee, including, but not limited to conviction of a felony, a crime of violence or a serious misdemeanor; and a record of arrests for continuing offenses, may be sufficient cause to deny or revoke staff-like access for that employee under the Task Order. Upon favorable completion of the final background investigation, the contractor employee is granted final access.

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. If NO, continue to Question 12.
The main data input into AQETL comes from two data extract files from IRS Form 720, and PRN files which is stored on the IRS BMF.

AQETL development and production servers rely on the Modernization Information Technology Services (MITS)-30 Wintel Application Servers General Support Systems (GSSs). AQETL also relies on the following MITS GSSs for infrastructure support:

- MITS-1 IRS Perimeter Security
- MITS-17 Enterprise Systems Domain
- MITS-26 Enterprise Remote Access (ERAP)
- MITS-30 Wintel Application Servers
- MITS-32 IRS Workstations and Support
- MITS-34 Enterprise Network

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

Business Master File (BMF)
- PIA completed 04/10/2007
- C&A completed 06/14/2007, expires 06/14/2010

MITS-1 IRS Perimeter Security
- PIA completed 02/16/2007
- C&A completed 09/25/2007, expires 09/25/2010

MITS-17 Enterprise Systems Domain
- PIA completed 02/27/2007
- C&A completed 09/27/2007, expires 09/27/2010

MITS-26 Enterprise Remote Access (ERAP)
- PIA completed 02/16/2007
- C&A completed 09/25/2007, expires 09/25/2010

MITS-30 Wintel Application Servers
- PIA completed 02/06/2007
- C&A completed 09/27/2007, expires 09/27/2010

MITS-32 IRS Workstations and Support
- PIA completed 01/11/2007
- C&A completed 09/21/2007, expires 09/21/2010

MITS-34 Enterprise Network
- PIA completed 01/22/2007
- C&A completed 09/25/2007, expires 09/25/2010

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?
AQETL has the capability to verify reports. All printed output is handled and secured in accordance with the IRS sensitive output handling organizational policy. AQETL has an established policy to retain data one year after it has been created. This is in accordance with IRM 1.15.2.9.

AQETL audit trail archival logs are retained for six (6) years, unless otherwise specified by a formal Records Retention Schedule developed in accordance with IRM 15.1, *Records Management.*

14. Will this system use technology in a new way? If "YES" describe. If "NO" go to Question
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.
N/A.

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 look at data to see and verify if it is in the right tax field. All AQETL users see the following warning banner upon logging in to the system:

> "THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!
> Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subject to criminal and civil penalties"

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.
No, this system will not 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?
N/A

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