

NOTE: The following reflects the information entered in the PIAMS website.

---

## A. SYSTEM DESCRIPTION

---

*Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management*

---

Date of Approval: February 10, 2014

PIA ID Number: **646**

---

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Automated Trust Fund Recovery, ATFR

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Not Applicable

---

## 4. Responsible Parties:

---

NA

---

## 5. General Business Purpose of System

---

The ATFR program is a National Standard Application (NSA) that was created to standardize several versions of the application. The application was designed and developed by Modernization and Information Technology Services (MITS) Headquarters and Applications Development in Austin, Texas. The application is in production at the Enterprise Computing Center – Memphis (ECC-MEM) in Memphis, Tennessee. ATFR computes trust fund amounts to aid Collections in making assessments on taxpayers who are officers in companies owing Trust Fund taxes. If a business has failed to collect or pay these taxes [e.g., Federal Insurance Contribution Act (FICA) and withholding] or has failed to pay collected excise taxes, the unpaid liability is assessed by ATFR against the responsible person(s). The application design divides the application into two programs: the Area Office (AO) and the Compliance Center (CC). ATFR-AO proposes assessments. The ATFR database receives case information weekly from two IRS systems: the Integrated Collection System (ICS) and the Integrated Data Retrieval System (IDRS). This case information identifies company records with a status of un-filed tax returns, or tax returns filed with a balance due. Specifically, ICS identifies the corporate Taxpayer Identification Numbers (TINs) for all flagged cases, and IDRS provides entity and module information for each case. Users of the AO component, Revenue Officers (RO), receive this information and complete a proposal for assessment to determine the person(s) responsible for the outstanding funds. The AO component uses an internal process to calculate the amount of funds due including any associated Trust Fund Recovery Penalties (TFRP). Once the responsible person(s) is identified, a form and letter (Forms 2751 and 1153) are sent to the responsible person(s) describing the proposed TFRP assessment. The responsible party may be not liable, liable but uncollectible (non-asserted), or fully/partially responsible. • If the responsible party is not liable, no action is taken • If the responsible party is liable but uncollectible, the RO will complete a Non-assertion Recommendation of Uncollectible TFRP (Form 9327) and a Recommendation for TFRP Assessment (Form 4183) and submit to his/her manager for approval • If the responsible party is fully or partially responsible, the responsible party can sign the Form 2751 to indicate agreement with the proposed assessment, waiving the 60-day appeals period. If the responsible party signs the Form 2751, the RO will complete a Request for TFRP Assessment (Form 2749) and transmit it to the ATFR-CC component immediately or when received within 60 days, and send a letter (Form 1155) to the responsible party acknowledging that the case will proceed to assessment. A Control Point Monitoring (CPM) user quality control process is performed prior to submission of a proposed assessment to the CC component. If the responsible party protests, then the RO will send the protested proposal to Appeals and further decisions will be made by Appeals, and the RO will send a letter (Form 1154) to the responsible party informing them that a protest was received and is being sent to Appeals for consideration Incoming payments for the assessments proposed by the AO component are received by IDRS. IDRS is updated with payments and sends information regarding the transaction in the form of a transcript to the CC component to alert the CC component that some activity has taken place. A synchronized monitor process (from the database server) checks for transaction postings within IDRS. The CC component performs the actual assessment of paid funds and cross-referencing of payments. A

preliminary automatic assessment is performed by CC to ensure that all received funds correspond with the proposed assessment (calculated by the AO component). If the case matches the assessment exactly (i.e. a case is completely paid within 60 days and there is no outstanding balance), a CC user does not need to review the case. If there is a discrepancy, the case is flagged and is required to be reviewed manually by a CC user (i.e. bankruptcy cases or errors such as IDRS is unavailable). The CC component will cross-reference any activities performed on an account (i.e. bounced check, partial payment, etc.). This function is necessary when a single payment is associated with several entities. The CC component will cross-reference the amount of the payment with each responsible entity to determine the appropriate credit to each entity, and transmit this data back to IDRS to update the IDRS records. The ATFR database holds taxpayer information and account information taken from IDRS. As stated above, a synchronized monitor process checks for transaction postings within IDRS. However, a refresh transaction will also manually update the database. Due process is administered outside the database pursuant to 26 USC .

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: April 26, 2011

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) Yes
- System is undergoing Security Assessment and Authorization Yes

6c. State any changes that have occurred to the system since the last PIA  
PIA is requested as part of eCM-r

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. N/A

**B. DATA CATEGORIZATION**

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	<u>Yes</u>		
Employees/Personnel/HR Systems	<u>Yes</u>		
Other	<u>No</u>	<u>Other Source:</u>	

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: Yes

<u>PII Name</u>	<u>On Public?</u>	<u>On Employee?</u>
Position in Company	Yes	No
Age	Yes	No

10a. What is the business purpose for collecting and using the SSN ?

ATFR only receives data that is required for the business purpose of the system. No “extra” data is imported. ATFR is designed to manage unpaid trust fund taxes from companies and officers. The use of the data in the system is both relevant and necessary to collect outstanding taxes owed by companies or their officers. When taxes are not collected from the company, ATFR then identifies which individual in the company is liable for the unpaid assessment.

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

26 USC 6109 is the authority for SSNs in IRS systems. 26 USC 6109 requires inclusion of identifying numbers in returns, statements, or other documents for securing proper identification of persons required to make such returns, statements, or documents.

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

NA

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

None planned

Describe the PII available in the system referred to in question 10 above.

The application design divides the application into two programs - the AO and the CC. A. Taxpayer: ATFR does store and process a subset of taxpayer information that is obtained from ICS and IDRS to contain TINs, and financial account information. The ATFR application contains the following taxpayer information: AO Program/CC Program • Company records with a status of un-filed tax returns • Tax returns filed with a balance due • Outstanding payment amount • Corporate TINs [i.e., Employee Identification Number (EIN), Social Security Number (SSN)] for flagged cases • Company name and name(s) of responsible company Officers • Module information for each case • Address, age and position within their company • Taxpayers fully or partially responsible to the assessment. (When a company does not respond to the assessments against it, the owners of the company or other responsible individuals are held personally accountable) • Amounts each taxpayer is responsible for paying or has paid toward the assessment • Financial account information • Status of unfiled cases B. Employee: During an employee’s term as an ATFR user, ATFR collects the following authenticating information about the employees for the AO program from Desktop Integration (DI). AO Program • Username • RO employee number • Standard Employee Identifier (SEID) • Email address • Phone number • Mailing address • Post of Duty (POD) address • Fax number • Telephone number • Badge number • Mailstop • Manager’s name CC Program • SEID • Password • Username • Tax examiner number • Role C. Audit Trail Information: The ATFR audit logs capture: • Date the event occurred • Unique Identifier • Type of event • Subject of event The ATFR database audit logs capture: • Date and time an event occurred • Server name • Process identification • Type of event, • Database instance, • User identification (ID) • Success/failure of the event A history log within ATFR-AO and ATFR-CC components records all user activities. The ATFR-AO History Table logs: • Date • Login ID • History text (description of the activity) The ATFR-CC History Table logs: • Corporate TIN • Creation Date (date case was created) • Date • Time • User code (User ID) • Status code (significant event that occurred) • Description (description of event) • Transcript date Audit trail records relevant to transactions obtained

from ICS and IDRS include the type of event, User ID, date; and TIN, Master File Table (MFT), and tax period, where applicable.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

The ATFR audit logs capture: • Date the event occurred • Unique Identifier • Type of event • Subject of event  
 The ATFR database audit logs capture: • Date and time an event occurred • Server name • Process identification  
 • Type of event, • Database instance, • User identification (ID) • Success/failure of the event A history log within ATFR-AO and ATFR-CC components records all user activities. The ATFR-AO History Table logs: • Date • Login ID • History text (description of the activity) The ATFR-CC History Table logs: • Corporate TIN • Creation Date (date case was created) • Date • Time • User code (User ID) • Status code (significant event that occurred) • Description (description of event) • Transcript date Audit trail records relevant to transactions obtained from ICS and IDRS include the type of event, User ID, date; and TIN, Master File Table (MFT), and tax period, where applicable.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

**System Name Current PIA? PIA Approval Date SA & A? Authorization Date**

ICS	Yes	10/24/2013	Yes	05/30/2011
AMS	Yes	03/16/2012	Yes	06/01/2012
IDRS	Yes	07/12/2011	Yes	10/09/2011

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): No

g. Other: No If **Yes**, *specify*.

### C. PURPOSE OF COLLECTION

*Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use*

13. What is the business need for the collection of PII in this system? Be specific.

ATFR only receives data that is required for the business purpose of the system. No "extra" data is imported. ATFR is designed to manage unpaid trust fund taxes from companies and officers. The use of the data in the system is both relevant and necessary to collect outstanding taxes owed by companies or their officers. When taxes are not collected from the company, ATFR then identifies which individual in the company is liable for the unpaid assessment.

### D. PII USAGE

*Authority: OMB M 03-22 & PVR #16, Acceptable Use*

14. What is the specific use(s) of the PII?

To conduct tax administration	<u>Yes</u>
To provide taxpayer services	<u>No</u>
To collect demographic data	<u>No</u>
For employee purposes	<u>No</u>



Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

If you answered yes to contractors, please answer **22a.** (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?

23. How is access to the PII determined and by whom?

ATFR CC Component: The login process to access the ATFR-CC module first requires the ATFR-CC user to successfully log into the ATFR-CC Windows via Remote Desktop Protocol server using his/her SEID and Directory Service password. The user is then presented with the ATFR-CC application, to which he/she must authenticate using his/her SEID and Oracle specific password for their Oracle account. ATFR AO Component: Identification & Authentication (I&A) for the ATFR-AO component is managed by AMS. The login process to access the ATFR-AO module requires the ATFR-AO user to successfully authenticate to an IDRS session, initiate an AMS session, and then double-click the ATFR icon for the ATFR-AO application. First, the user must sign-in to an IDRS session with the IDRS login prompt, from an InfoConnect Session file on the user's desktop. Then, the user must initiate an AMS session, when the user double clicks on the AMS icon, while successfully authenticated into IDRS. (The user does not have to separately login to AMS as well). Once the ATFR-Web component is selected from the AMS menu, the user is taken to the ATFR-Web application. At the application level, ATFR enforces assigned authorizations through role-based access. The user roles within the ATFR-AO and ATFR-CC components are created based on a managed hierarchy. This allows for each user role to be monitored by a more supervisory role. The use of "superuser" privileges is limited to System Administrators and Database Administrators and all actions are audited. A "superuser" account has "root" access to the operating system, affording access to all system administration and security functions. Application developers (contractors) do not have access to the production system or production data.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

Checks for accuracy, completeness, and validity of information are accomplished by the application and guided by the business requirements. Information input consists of pre-defined drop-down lists and user required input. The pre-defined drop-down lists are implemented for all fields that lend themselves to prepared data. For manual input, the data is checked for valid syntax (e.g., character set, length, numerical range, acceptable values) and will be validated to ensure that inputs match specified definitions for format and content. For data imported from other systems, ATFR is dependent upon the validity checks that are completed for data input in those systems.

25. 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

25a. 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.

All Automated Trust Fund Recovery (ATFR) data is maintained on the ATFR database at ECC-MEM. ATFR Area Office segment of the application, which proposes the assessment was fully deployed nationwide October 2000. Procedures are documented in the IRM 5.7.6.6 Collections, regarding Collections Statute Expiration Date (CSED). IRM 5.7.6.6 (1) TFRP case files are maintained in the Control Point Monitoring unit in Technical Services - Advisory for two years after the assessment. After two years the files are sent to the Federal Records Center where they are destroyed 12 years after assessment (this allows for the CSED plus 2 years for the taxpayer to file a claim for refund) in accordance with Records Control Schedule (RCS) 28 for Collection, Item 41(c). ATFR data is approved for destruction under RCS 35 for Tax Administration Electronic Systems, Item 34, when one year old or when no longer needed for administrative, legal, audit or other operational purposes, whichever is sooner. The Records Office and SB/SE agree, however, this might be in error and/or in need of an update as the current disposition instructions do not allow for the maintenance of ATFR system data for extenuating circumstances ongoing after one

year. The Records Office and SB/SE will work together to resolve any records scheduling issues and will draft an updated request for records disposition authority for submission to/approval by the National Archives and Records Administration, if necessary. NOTE: IRS Records Control Schedules (RCS) have been re-published or are in the process of transitioning from an IRM publication format to publication in one of two RCS Documents. Former IRMs 1.15.8-37 are re-published as RCS 8-37 in Document 12990, and former IRMs 1.15.38-64 are re-published as RCS 38-64 in Document 12829.

If **No**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

- 
26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

The ATFR user interface is physically separated from the ATFR database server. The application (ATFR-AO and ATFR-CC) and the database reside on separate servers. In addition, ATFR application users do not have direct access to the data in the ATFR database. ATFR CC Component: The login process to access the ATFR-CC module first requires the ATFR-CC user to successfully log into the ATFR-CC Windows via Remote Desktop Protocol server using his/her SEID and Directory Service password. The user is then presented with the ATFR-CC application, to which he/she must authenticate using his/her SEID and Oracle specific password for their Oracle account. ATFR AO Component: Identification & Authentication (I&A) for the ATFR-AO component is managed by AMS. The login process to access the ATFR-AO module requires the ATFR-AO user to successfully authenticate to an IDRS session, initiate an AMS session, and then double-click the ATFR icon for the ATFR-AO application. First, the user must sign-in to an IDRS session with the IDRS login prompt, from an InfoConnect Session file on the user's desktop. Then, the user must initiate an AMS session, when the user double clicks on the AMS icon, while successfully authenticated into IDRS. (The user does not have to separately login to AMS as well). Once the ATFR-Web component is selected from the AMS menu, the user is taken to the ATFR-Web application. At the application level, ATFR enforces assigned authorizations through role-based access. The user roles within the ATFR-AO and ATFR-CC components are created based on a managed hierarchy. This allows for each user role to be monitored by a more supervisory role. The use of "superuser" privileges is limited to System Administrators and Database Administrators and all actions are audited. A "superuser" account has "root" access to the operating system, affording access to all system administration and security functions. Application developers (contractors) do not have access to the production system or production data.

- 26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

The ATFR application protects the confidentiality and integrity of information at rest. No SBU data is stored on a user's laptop. All user laptops are encrypted using EDE. The application also utilizes Windows file encryption (EFS). All information sent from other applications to the ATFR application is encrypted. In addition, the ATFR application establishes and manages cryptographic keys for required cryptography as the ATFR Oracle DBMS connection is encrypted between client and database. The use of cryptography on IRS information systems is documented in IRM 10.8.1. The IRM states that: \* All IRS information systems perform all cryptographic operations (including key generation) using FIPS 140-2 or later validated cryptographic modules operating in approved modes of operation; \* IRS organizations with sensitive encryption applications under their authority develop encryption plans for all IT systems; and \* IRS submits an encryption plan to the Treasury for approval before implementation. The Oracle database encrypts ATFR-CC user passwords using an encryption algorithm intrinsic to Oracle. The integrity of all transmitted information is protected and encrypted through the use of EFTU and unique identification and authentication into the application. All user workstations are encrypted and the application's database encrypts information between the client and database. The ATFR application employs cryptographic mechanisms to ensure recognition of changes to information during transmission as the ATFR Oracle DBMS connection is encrypted between client and database.

- 
27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

- 
28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

eCM, eCM-r completed on an annual basis

---

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

---

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate*)?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

---

## H. PRIVACY ACT & SYSTEM OF RECORDS

---

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

*Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency*

---

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

---

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORN Number	SORN Name
24.030	CADE Individual Master File (IMF)
24.046	CADE Business Master File (BMF)
26.013	Trust Fund Recovery Cases/ One Hundred Percent Pen
26.019	Taxpayer Delinquent Account (TDA) Files
34.037	Audit Trail and Security Records

## I. ANALYSIS

*Authority: OMB M 03-22 & PVR #21- Privacy Risk Management*

---

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

32a. If **Yes** to any of the above, please describe:

NA