

Date of Approval: **January 27, 2020**

PIA ID Number: **4617**

SYSTEM DESCRIPTION

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

Automated Trust Fund Recovery, ATFR

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 Trust Fund Recovery (ATFR) #2102 Operation & Maintenance

What is the approval date of the most recent PCLIA?

2/22/2017

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.

Small Business/Self Employed (SBSE) Governance Board

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.

The Automated Trust Fund Recovery (ATFR) program was created to standardize several versions of the application. 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 CC component performs the actual assessment of unpaid trust fund amounts and cross-referencing of payments. The ATFR database holds taxpayer information and account information taken from Integrated Data Retrieval System (IDRS).

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

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

The Office of Management and Budget memorandum Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The ATFR system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. SSNs are redacted from correspondence items.

Employer Identification Number

Other Taxpayer 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

Phone Numbers

E-mail 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

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

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.

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 their 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.

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

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.

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 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 26.013 Trust Fund Recovery Cases/One Hundred Percent Penalty Cases

IRS 26.019 Taxpayer Delinquent Account Files

IRS 34.037 Audit Trail and Security Records

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: Business Master File Accounts Data Store (BMF DS)
Current PCLIA: Yes
Approval Date: 8/27/2018
SA&A: Yes
ATO/IATO Date: 2/28/2019

System Name: Individual Master File On-Line (IMFOL)
Current PCLIA: Yes
Approval Date: 3/6/2017
SA&A: Yes
ATO/IATO Date: 10/3/2019

System Name: National Account Profile (NAP)
Current PCLIA: Yes
Approval Date: 3/21/2017
SA&A: Yes
ATO/IATO Date: 8/4/2012

System Name: Taxpayer Information File Data Store (TIF DS)
Current PCLIA: No
SA&A: No

System Name: Centralized Authorization File (CAF)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: No

System Name: Integrated Collection System Mainframe (ICS)
Current PCLIA: Yes
Approval Date: 5/14/2019
SA&A: Yes
ATO/IATO Date: 5/2/2019

System Name: Data Master-1 (DM-1 DS)
Current PCLIA: No
SA&A: No

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?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Integrated Collection System Mainframe (ICS)

Current PCLIA: Yes

Approval Date: 5/14/2019

SA&A: Yes

ATO/IATO Date: 5/2/2019

System Name: General Updates (GEN UP)

Current PCLIA: No

SA&A: No

System Name: Business Master File Outputs (BMF OUTPUTS)

Current PCLIA: Yes

Approval Date: 3/8/2018

SA&A: Yes

ATO/IATO Date: 11/12/2019

System Name: Integrated Data Retrieval System (IDRS) - Taxpayer Delinquent Account (TDA)

Current PCLIA: Yes

Approval Date: 10/1/2018

SA&A: Yes

ATO/IATO Date: 10/28/2019

Identify the authority

ATFR sends case related data to Integrated Collection System (ICS). Data includes case actions taken within ATFR relevant to the business entity case assigned to the Revenue Officers on ICS. Actions taken include generation of forms and correspondence related to Trust Fund Recovery Penalty (TFRP) case processing. ATFR also sends case data related to assessments to Integrated Data Retrieval System (IDRS).

For what purpose?

Actions taken include generation of forms and correspondence related to Trust Fund Recovery Penalty (TFRP) case processing.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

All individuals have the right to decline to provide information. However, they may be subject to Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

All individuals have the right to decline to provide information. However, they may be subject to Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

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

Regarding the Trust Fund Recovery Penalty and the ATFR application, taxpayers are afforded due process rights when they are issued the Letter 1153, Proposed Trust Fund Recovery Penalty Notification. The Letter 1153 provides the taxpayer with the right to file suit in the U.S. District Court or the U.S. Court of Federal Claims. The Letter 1153 provides the taxpayer with the opportunity to provide additional information and/or state their case regarding the proposed Trust Fund Recovery Penalty assessment. The delivery date of the Letter 1153 is logged into ATFR. If a Form 4180 interview is conducted, the interviewee is provided with Notice 609, Privacy Act Notice.

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 Write

Managers: Read Write

System Administrators: Read Write

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

Access to ATFR is controlled using the OL5081 approval process. 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.

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.

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 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 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 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.

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?

4/16/2019

Describe the system's audit trail.

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.

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)?

The Annual Security Control Assessment (ASCA) test results are stored on the Treasury "FISMA: Federal Information Security Management Act) Inventory Management System (TFIMS).

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?

ASCA testing will begin in March 2020.

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: Not Applicable

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?

No

Does computer matching occur?

No

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