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: August 1, 2014 PIA ID Number: **890**

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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

Fraud Inventory Management System, FIMS

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:	Under 100,000

4. Responsible Parties:

N/A

5. General Business Purpose of System

This is a resubmission of a PIA originally approved by the Office of Privacy in 2009. The system is used as an organization tool for Fraud Technical Advisors to record the cases they are involved in on an advisory capacity. This is a tool where the Fraud Technical Advisor keep track of the numerous contacts with the compliance employee assigned to the case and pertinent dates as the case progresses through the developmental stages. It contains the date of any significant case activity including meetings with the examiner, what was discussed and or determined. Due process is provided pursuant to 26 USC, 18 USC, and 31 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: 3/26/2009 12:00:00 AM

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) No
- System is undergoing Security Assessment and Authorization No

6c. State any changes that have occurred to the system since the last PIA

No Changes have occurred.

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'. none

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	No	
Employees/Personnel/HR Systems	Yes	
		Other Source:
Other	No	

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	No	No	No
Date of Birth	No	No	No

Additional Types of PII: No

No Other PII Records found.

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

SSN collected on taxpayers to use to support tax administration to match and verify with other IRS inventory systems (such as IDRS, ERCS, ENTITY) that may be used to research taxpayer account information.

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.)

IRC Section 6109

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

None being considered at this time.

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

Not currently being considered.

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

Taxpayer name, SSN and/or ITIN collected on taxpayers to use to support tax administration to match and verify with other IRS inventory systems (such as IDRS, ERCS, ENTITY) that may be used to research taxpayer account information. Compliance employee name, work phone number, compliance employee group manger name and Special Agent name is needed to allow FTA to make periodic follow up contacts while assisting with case development. All information is entered into the program by the FTA. No electronic data import or population. The program is stand alone and does not communicate

with other programs.

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.

There is no audit trail

12. What are the sources of the PII in the system? Please indicate specific sources:
    a. IRS files and databases: No
    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.

The data is collected to record a case history and contacts of the Fraud Technical Advisor working with the compliance employee to assist in case development of potential fraud cases. This data allows Fraud Technical Advisors to accurately and timely manage their inventory and provide timely cases assistance and follow-ups to the compliance employees.

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	Yes	
To provide taxpayer services	No	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?
    If yes, please indicate means:

	YES/NO	**AUTHORITY**
Persistent Cookies		
Web Beacons		

Session Cookies

If other, specify:

Other:

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

No decision that would be the basis for legal or administrative action is intended to come from data in this system. In the extremely unlikely situation where basis for legal or administrative action may result due to incorrect system data, the system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

ID Form Number Form Name

- 3723 1040 Individual Income Tax Return
- 3724 1120 Corporate Income Tax Return
- 3725 990 Return of Organization Exempt from Income Tax
- 3733 1120S U.S. Income Tax Return for an S Corporation
- 3734 8300 Report of Cash Payments Over $10,000 Received In a Trade or Business
- 3735 1065 U.S. Return of Partnership Income
- 3736 940 Employer's Annual Federal Unemployment (FUTA) Tax Return
- 3737 941 Employer's Quarterly Federal Tax Return

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Write
Managers		No Access
System Administrators		No Access
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

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

This database resides on the Fraud Technical Advisor's computer in an encrypted folder. Fraud Technical Advisors (IRS employees) input and have access to PII. Each FTA can only access PII for cases they are assisting with.

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

FTAs input the PII data based on information received from Compliance employees. No other verification steps occur.

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.

FTA data is scheduled under National Archives Job No. N1-58-09-6. Data is maintained for 3 years after closure. A closed case for this purpose consists of the later of 1) the conclusion of FTA involvement, 2) the conclusion of the related criminal case, or 3) the conclusion of any civil litigation related to the fraud issues. These disposition instructions are published in Document 12990 under Records Control Schedule (RCS) 28 for Tax Administration - Collection, item 6a1.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
PII data is secured on each users IRS issued laptop. Program data is secured in SBU encrypted folders.

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

Data is secured by standard IRS software and hardware security and encryption policies and procedures. Employees are expected to follow all IRS/IRM safeguards to protect data and equipment at rest, in flight or in transition.

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? No

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

No unique monitoring/evaluating activities for this system. Employees do take annual IT/Security briefing updates.

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

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.

Treas/IRS 42.001	Exam administrative records
Treas/IRS 34.037	IRS audit trail and security records system
Treas/IRS 24.030	IMF
Treas/IRS 24.046	BMF

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)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	Yes
Other:	No

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

We are considering the feasibility of truncating the SSNs.