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: Jun 24 2014 12:00am PIA ID Number: **954**

1. What type of system is this? Legacy

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

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

Taxpayer Advocate Management Information System, TAMIS

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:	Under 5,000
Members of the Public:	Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

TAMIS is the principal database of the National Taxpayer Advocate (NTA) and the Taxpayer Advocate Service (TAS). It is an automated, computerized application used to record, control, process, analyze and report on TAS case inventories involving taxpayers who experience significant hardship or other tax account problems caused by the Service's administration of the tax laws, other IRS systemic processes and policies or the tax laws themselves; and who request Taxpayer Advocate relief or assistance in resolving their concerns. Advocate authority and responsibility to consider and act upon taxpayer significant hardship and other tax-related problems and to grant the appropriate relief or assistance is statutorily established by IRC Sections 7803 (c) (2) (A) (i) and 7811. TAMIS is used by TAS personnel and caseworkers to record, manage, process, and resolve all taxpayer cases and issues that fall within the Advocate's jurisdiction. Due process is provided 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: 02/17/2012

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 Yes

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

N/A

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'. 015-45-01-13-02-2134-00

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

8a. If **No**, what types of information does the system collect, display, store, maintain or disseminate?

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	Yes	
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	Yes
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	Yes
Date of Birth	Yes	Yes	No

Additional Types of PII: Yes

PII Name	**On Public?**	**On Employee?**
Phone Number	Yes	Yes
Spouse Name	Yes	No
Spouse SSN	Yes	No

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

SSN on Taxpayer's, their spouses, and dependents is stored when relevant to the issue. The TIN of the primary taxpayer is required for each case in the system in order to properly identify the individual applicable to the case.

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 Sections 6103 and 7803.

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

TAMIS cannot completely eliminate the use of SSN within the application; however, SSN masking is employed for outgoing letters to taxpayers. The SSN is required in order to properly identify the individual applicable to the case.

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

A new system is in development to replace the TAMIS application. This system, Taxpayer Advocate Service Integrated System (TASIS), will limit the dependency on the individual's SSN. TASIS mitigates the SSN usage on the system by not requiring manual input on the system. TASIS will rely on interdependent IRS applications to provide this information.

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

The TAMIS application collects an individual's name depending on the nature of the tax return. The name of IRS employees is stored regardless of the type of tax return generated. For members of the public, spouses names are collected in cases where a joint tax return is submitted. SSN on Taxpayer's, their spouses, and dependents is stored when relevant to the issue. Some PII items are required depending on the case. The TIN of the primary taxpayer is required for each case in the system. Individual Taxpayer Identification Numbers (ITINs), Adoption Taxpayer Identification Numbers (ATINs), and Preparer Taxpayer Identification Numbers (PTINs) are collected when required to address the issue entered into the system. Date of birth is collected on members of the public as needed. SEIDs are stored for all employees within the TAMIS system. The public phone numbers stored in the system could be home, business, or other. Employee phone numbers are limited to the business only.

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.

Within the TAMIS application two tables provide most of the audit trail information. The audit log table records actions taken (user action), who performed the action (user_emp_id), on what case the action was taken (case number, or employee identification (ID) if the action was to the employee table), and when the action was taken (date stamp). The audit changes table records the before and after values of any changed field; the audit sequence joins the audit changes table to the master record in the audit log table. The audit (table name) tables hold copies of records from their counterpart tables when a record is deleted. Outside of the TAMIS application, the Sun platform will provide additional audit trail information and will be the responsibility of systems administration there. Employee login information will include who logged, when, for how long, and what processes were run during each session.

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
Account Management Services (AMS)	Yes	11/10/2009	Yes	08/03/2009
Account Management Services (AMS)	Yes	11/10/2009	Yes	08/03/2009

b. Other federal agency or agencies: No

If **Yes**, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If **Yes**, please list the agency (or agencies) below:

d. Third party sources: Yes

If yes, the third party sources that were used are:

Taxpayers or individuals who initiate correspondence on behalf of a taxpayer such as a power of attorney and other third parties, including financial institutions, suppliers, and other vendors, as required to resolve the taxpayer's case.

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

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.

TAMIS is used by TAS personnel and caseworkers to record, manage, process, and resolve all taxpayer cases and issues that fall within the Advocate's jurisdiction.

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 Yes

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.) Yes

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	No		
State and local agency (-ies)	No		
Third party sources	No		
Other:	Yes	Congress	

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

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? Yes

18a. If **Yes**, how is their permission granted?

Individuals can verbally opt-out or refuse to respond for more information.

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”?

The system will allow affective 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.

No forms found.

20b. If **No**, how was consent granted?

Written consent ____________

Website Opt In or Out option ____________

Published System of Records Notice in the Federal Register ____________

Other: ____________

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

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

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		Read Write
System Administrators		No Access
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other: TIGTA	Yes	Read Only

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?

A user's manager must submit an On-Line 5081 (OL5081) for an individual to obtain access.

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

The TAS caseworker is in contact with the taxpayer or the taxpayer representative and requests supporting documentation for the case then verifies information received with what IRS systems show for the taxpayer. The taxpayer will provide feedback if the information is not accurate or missing since the proposed resolution of the case will not be acceptable. Caseworker reviews, managerial reviews, and quality reviews will also identify areas of concern. Timeliness is ensured through contact with the taxpayer or taxpayer representative. TAS caseworkers verify data received from the taxpayer or the taxpayer representative against the records of IRS has for that taxpayer. This data either helps solve the taxpayer's problem, helps determine if the problem is the taxpayer's or the IRS fault, or helps identify processing problems within the IRS.

---

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.

TAMIS case management data is approved for destruction three years after case is closed (Job No. N1-58-09-81, approved 12/1/09). Disposition instructions are published in IRS Document 12990 under Records Control Schedule (RCS) 9 for Taxpayer Advocate, Item 94. To archive TAMIS case data the TAMIS System Administrator at the Detroit Computing Center (DCC) executes an archive script from a shell prompt. When the retention period expires for data stored on tape, the tape will be demagnetized and put back in circulation for reuse. These procedures are outlined in the TAMIS Application System Security Plan.

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 TAMIS application is internal to the IRS only. Employees are prohibited from extracting information and distributing from outside the IRS. UNAX requirements are also leveraged to protect the data within the application. Secure messaging is required when information is transmitted within the IRS firewall. TAMIS uses audit trails as required by IRS 2.1.10, Information Systems Security, May 1998, and a Functional Security Coordinator is assigned. All employees are required to attend UNAX Training and they have been trained on the use of the system and their responsibilities concerning access and use of the data. Users are forbidden to access, research, or change any account, file, record, or application that is not required to perform official duties. Users are restricted to accessing, researching, or changing only accounts, files, records, or applications that are required to perform their official duties. Users are restricted from accessing their individual/spouse account, accounts of relatives, friends, neighbors, or any account in which the user has a personal or financial interest. Users are restricted from accessing the accounts of a famous or public person unless given authorization to do so. If asked to access an account or other sensitive or private information, users are required to verify that the request is authorized and valid. TAMIS User permissions are granted based on least privilege. The program contains a number of access levels for users based upon their necessary function within the organization. Users with an access level of 0 are query/view only. Users with an access level of 1 are limited case workers and can only query/view cases and edit cases assigned within their org code. Users with an access level of 2 are considered full case workers and have the ability to query/view, add, and edit cases assigned to them or cases within their org code. Users with an access level of 3 are TAS Managers, they have full access to cases and can update employee records belonging only to their own assigned org code. Users with an access level of 4 are TA & TA Staff, they can update employee records belonging only to their own assigned organization code Users with access level of 5 can update employee records belonging to any organization code. Level Full Access allows a user to add/update information as it necessary and to compose letters and generate reports/listings.

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

The TAMIS application is internal to the IRS only. Employees are prohibited from extracting information and distributing from outside the IRS. UNAX requirements are also leveraged to protect the data within the application. Secure messaging is required when information is transmitted within the IRS firewall. TAMIS uses audit trails as required by IRS 2.1.10, Information Systems Security, May 1998, and a Functional Security Coordinator is assigned. All employees are required to attend UNAX Training and they have been trained on the use of the system and their responsibilities concerning access and use of the data. Users are forbidden to access, research, or change any account, file, record, or application that is not required to perform official duties. Users are restricted to accessing, researching, or changing only accounts, files, records, or applications that are required to perform their official duties. Users are restricted from accessing their individual/spouse account, accounts of relatives, friends, neighbors, or any account in which the user has a personal or financial interest. Users are restricted from accessing the accounts of a famous or public person unless given authorization to do so. If asked to access an account or other sensitive or private information, users are required to verify that the request is authorized and valid. TAMIS User permissions are granted based on least privilege. The program contains a number of access levels for users based upon their necessary function within the organization. Users with an access level of 0 are query/view only. Users with an access level of 1 are limited case workers and can only query/view cases and edit cases assigned within their org code. Users with an access level of 2 are considered full case workers and have the ability to query/view, add, and edit cases assigned to them or cases within their org code. Users with an access level of 3 are TAS Managers, they have full access to cases and can update employee records belonging only to their own assigned org code. Users with an access level of 4 are TA & TA Staff, they can update employee records belonging only to their own assigned organization code Users with access level of 5 can update employee records belonging to any organization code. Level Full Access allows a user to add/update information as it necessary and to compose letters and generate reports/listings.

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.

Management utilizes Business Objects Audit Reports to monitor and evaluate user activities and to safeguard PII data within the system. Managerial reviews occur on a biweekly basis. In addition, various managerial case reviews are conducted to monitor and evaluate TAMIS user actions on a case by case basis. These reviews include early intervention, 60 day, 100 day, pre-closure, and workload.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

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

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

01/29/2014

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.

SORNS Number	**SORNS Name**
00.003	Taxpayer Advocate Service and Customer Feedback an
34.037	IRS Audit Trail and Security Records System

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 No

Other: No

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

NA