

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: Apr 11 2014 12:00AM

PIA ID Number: **826**

1. What type of system is this? New

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 Service Integrated System, TESIS

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

In support of the managing taxpayer accounts (MTA) domain transitional architecture, the Taxpayer Advocate Service Integrated System (TASIS) provides a unified system that enhances the ability of Taxpayer Advocate Service (TAS) to help taxpayers resolve problems with the IRS and recommend changes to prevent the problems. TASIS seeks to establish a common platform, leveraging existing database functionality and new IRS standards in electronic document management, data management, and portal strategies. In addition, TASIS will reuse common services developed and provided by other IRS initiatives consistent with the overall IRS Service Oriented Architecture (SOA) strategy. TASIS will replace the Taxpayer Advocate Management Information System (TAMIS), Systemic Advocacy Management System II (SAMS II), and several MS-Access databases. TASIS also utilizes the Business Objects Enterprise (BOE) to provide TASIS users the ability to generate reports. BOE is a Commercial off the Shelf (COTS) product and resides on the GSS-24 UNIX Consolidated Platform. BOE administration and security responsibilities are provided by GSS-24 and are not considered part of the TASIS boundary. BOE is physically located on a separate server and is used by multiple applications. TASIS stores documents and information pertaining to those documents on Documentum. 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: 07/13/2011

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) No
 - System is undergoing Security Assessment and Authorization Yes
-

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

TASIS is in development and targeted for deployment by 12/19/2014. The application has advanced from one MS2 to MS3-4a.

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'. 015-45-01-13-02-2555-00

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	<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	Yes
Social Security Number (SSN)	Yes	Yes	Yes
Tax Payer ID Number (TIN)	Yes	Yes	Yes
Address	Yes	Yes	Yes
Date of Birth	Yes	Yes	Yes

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Telephone number	Yes	Yes
Spouses 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.

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.)

SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. Additional information can be found at these two links: • <http://www.irs.gov/pub/irs-wd/00-0075.pdf> • <http://www.law.cornell.edu/uscode/text/26/6109> Section 7801 and 7803 of the Internal Revenue Code.

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

IRS and Congress have not provided for an alternative means to identify taxpayers

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

No strategy exists currently for the application.

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

The TESIS 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 TESIS 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 TESIS 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 TESIS application, the Linux environment 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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
IDRS	Yes	07/21/2011	Yes	12/09/2011
AMS	Yes	03/16/2012	Yes	06/01/2012
IDRS	Yes	07/21/2011	Yes	12/09/2011
AMS	Yes	03/16/2012	Yes	06/01/2012

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.

TASIS 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	_____	_____
Other:	_____	<i>If other, specify:</i> _____

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?

The individual can determine not to submit an E911 request for TAS assistance.

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

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

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:	<u>Yes</u>	
Users		Read Write
Managers		Read Write
System Administrators		No Access
Developers		No Access
Contractors:	<u>No</u>	
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?

Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user be added. They must fill out an OL5081, Information System User Registration/Change Request, to request access to the application. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on OL5081. TESIS will exercise authorities granted via Internal Revenue Code (IRC) 7803.

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

The TESIS caseworker is in contact with the taxpayer or the taxpayer representative and requests supporting documentation for the case. The caseworker 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. TESIS 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.

TESIS is a new IRS TAS application in development. It will replace the Taxpayer Advocate Management Information System (TAMIS), the Systemic Advocacy Management System II (SAMS II), and several MS-Access databases. In advance of its 2014 operational date, TAS and the IRS Records Office are working together to draft and submit to the National Archives and Records Administration (NARA) a request for records disposition authority that will provide mandatory retentions for TESIS inputs, system data, outputs and system documentation. When approved by NARA, TESIS disposition instructions will be published in IRM 1.15.9 (Records Control Schedule (RCS) for Taxpayer Advocate...soon to be re-published in Document 12990 as simply RCS 9), item number to be determined.

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.

A web service is currently being developed for TESIS and will use secure https when transferring data. HTTPS signals the browser to use an added encryption layer of Secure Sockets Layer (SSL) to protect the traffic. SSL uses the RSA (Rivest, Shamir and Adleman) encryption module, which is an asymmetric key algorithm (private/public).

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

TESIS relies upon GSS-42 for securing PII data at rest. The GSS-42 GSS protects TESIS data at rest as follows: Back Up Tapes: GSS-42 uses the IRS Veritas Netbackup Solution for tape backup. Veritas encrypts all backup tapes utilizing FIPS 140-2 validated encryption. Application Servers: IRM 10.8.1.5.4.6 (15) states that encryption of data residing on the primary stored devices of IRS information systems (e.g., servers, mainframes) is not required. The GSS-42 environment, in accordance with the IRM, has employed the following due diligence methods for

protecting the TESIS PII data that resides on the servers: TESIS does not utilize any shares or shared drives. TESIS enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties. TESIS does not routinely print any documents. If required, printing is limited to the specific reason for printing any document. TESIS has had a risk assessment conducted. Security Assessment Services has previously completed a Security Impact Analysis and will conduct a new SIA as part of the current SA&A cycle. The TESIS SSP is being updated as part of the current SA&A to reflect the encryption utilized by GSS-42 environment to protect PII data. Physical security is an inherited control by TESIS at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan.

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.

Continuous Monitoring (eCM) is performed annually to determine if selected System Security Plan (SSP) controls are operating as intended. This process is conducted annually on a three year cycle whereby all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the eCM are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

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?

12/19/2012

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

Treasury IRS 00.003 Taxpayer Advocate Service and Customer Feedback an

Treasury IRS 34.037 IRS Audit Trail and Security Records System

Treasury IRS 00.001 Correspondence Files and Correspondence Control Fi

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