

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: Oct 15 2014

PIA ID Number: **709**

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):

Systemic Advocacy Management System, Generation 2, SAMS II

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

The Systemic Advocacy Management System II, Release 3.2 (SAMS II) is a National Taxpayer Advocate Service (TAS) application that acts as the primary method of receiving and prioritizing systemic issues and problems submitted by IRS employees and the general public. As an independent organization within the IRS, TAS employs SAMS II to facilitate taxpayers' ability to submit issues, suggestions, and ideas to help reduce or eliminate the burdens facing taxpayers. The TAS Office of Systemic Advocacy utilizes SAMS II to record analysis of submitted issues and reviewer recommendations for follow up. SAMS II includes advocacy projects developed from selected submissions. SAMS II allows Systemic Advocacy to quickly identify tax administration problems; monitor and analyze trends; respond to problems through projects; and, when appropriate, channel the most serious problems into the National Taxpayer Advocate's Annual Report to Congress. TAS also documents several other systemic-level advocacy efforts. This includes reviews of internal management documents (IMD), participation on cross functional task force teams, "portfolio" or subject matter expert assignments, and Annual Report to Congress topics (both development assignments and monitoring of IRS actions on recommendations). SAMS II allows taxpayers, practitioners, businesses, professional groups, and academic institutions to submit systemic issues through IRS.gov directly to the Office of Systemic Advocacy, a branch of TAS. For example, a taxpayer receives a refund in the amount of \$15,000 instead of \$1,500 and suspects a faulty computer program. The taxpayer would then complete the web form at <http://www.irs.gov/advocate>. This information from the taxpayer's forms is compiled on a daily basis to an XML file. Administrators download the XML file via File Transfer Protocol (FTP) to their desktop. Administrators then utilize an executable script to upload the information to the SAMS database. Encrypted data (256 bytes) is sent to the web services interface and is then decrypted, verified and passed to the application for processing. The only identity information retained with an issue submitted through IRS.gov is an e-mail address. Submissions from within the IRS network will pull the employee's contact information from the Active Directory unless the employee elects to remain anonymous. Data within SAMS II includes records of: a.) Possible tax law or tax administration problems/opportunities that impact groups of taxpayers and b.) Efforts to correct or proactively avoid such problems. SAMS II requests the individual submitting an issue through IRS.gov to provide an email address for acknowledgement or possible follow-up but does not request any other form of Personally Identifiable Information (PII). Office contact information (Name, office address, office telephone, e-mail address, and Standard Employee Identifier (SEID) is retained for all authorized users, program contacts, and internal submitters – excluding submitters selecting anonymity. PII maintained in the SAMS II system includes the submitter provided email address and employee contact information stated above. Additionally, names, addresses and phone numbers of external submitters are also maintained if this information is voluntarily provided during subsequent contacts. SAMS II does not contain Taxpayer Identification Numbers (TIN), therefore Negative TIN checking is not applicable this application. SAMS II utilizes Business Objects as its reporting application. Read-only reports are passed to the Business Performance Management System (BPMS) where data is maintained for statistical purposes.

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: 11/10/2011 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
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'. 015-45-01-13-02-2515-00

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>	<i>Other Source:</i> _____

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: No

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

Each data item is necessary to prioritize and resolve systemic issues and problems submitted by IRS employees and the general public and to provide status updates to taxpayers. The data is also needed to help facilitate taxpayers' ability to submit issues, suggestions, and ideas to help reduce or eliminate the burdens facing taxpayers.

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)

SAMS cannot completely eliminate the use of the TIN; however, TIN masking is employed for outgoing letters. The TIN may be required to properly identify individuals applicable to the systemic issue.

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

The SAMS application does not have a dependency on TINs. TINs are not utilized in every issue, just those issues where specific taxpayer information is needed to resolve the systemic issue.

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

Taxpayer: Names Home or email addresses Telephone numbers Social Security Numbers Date and place of birth Tax return or salary information Employee: SEID Name Office Telephone Number Email Address Physical Address Other: If the SAMS II Program Management Office (PMO) was to contact someone from an outside agency regarding interrelated processes, the following information would be manually entered into the SAMS application by an IRS employee: Other Federal Agencies Office Contact Information: Name Office Telephone number E-mail address Physical address State and Local Agencies Office Contact Information: Name Office Telephone number E-mail address Physical address

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 SAMS application, all changes are recorded. The Audit table contains all the "before" values while the current table holds and displays current data. All changes shown in the Audit table contains the date and time of the change and who made the change. The Audit table contains information about who is given access, their roles and any changes to the users profile and who made the change. The SAMS application does not record when a user accesses the system or an issue; nor does it record the amount of time logged into the system or an issue.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

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

a. IRS files and databases: No

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

No System Records found.

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:

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?

verbally, through communication with the Systemic Analyst.

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? No

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

Written consent	<u>Yes</u>
Website Opt In or Out option	<u>No</u>
Published System of Records Notice in the Federal Register	<u>No</u>
Other: <u>verbal</u>	<u>Yes</u>

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		<u>Read Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>No Access</u>
Developers		<u>No Access</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u>Read Only</u>

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 TAS program office. Completion of a formal request via OL5081 containing the appropriate electronic signature and manager's approval are needed prior to receiving a system account. Additional controls include restriction of user access based on job functions and responsibilities, "need-to-know" and

separation of duties. Users are assigned to groups that are permitted to access specific data dependent on job functions, systemic issue project roles and responsibilities. Contractors must complete a background investigation. Access is restricted to development environment. Contractors may view user contact data imported from the Corporate Authoritative Directory Service and similarly available to them on the Global Address List with network access.

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

SAMS II relies on the user (e.g., employee, general public) of the system to enter accurate information. Several fields within the application require information input validation or limit data inaccuracies by using a drop-down list.

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.

SAMS II data is approved for destruction 10 years after removal to Archives storage. In accordance with disposition instructions approved by the National Archives and Records Administration (NARA) under Job No. N1-58-08-3, data for last 10 fiscal years of all issue submissions and associated projects are to be retained in SAMS II Active database. Issue and closed project data are to be moved to Archives 10 years after they were received, and subsequently deleted from Archives after an additional 10 years. These data disposition instructions, along with dispositions approved for SAMS II inputs, outputs and system documentation are published in Document 12990 under Records Control Schedule (RCS) 9 for Taxpayer Advocate, item 95.

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 SAMS application is internal to the IRS only. Users of the system remove any PII that would be available to those without an OL5081. The SAMS 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. 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. SAMS User permissions are granted based on least privilege. The program contains a number of roles and users are assigned those roles based upon their function within the organization and the application.

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

The SAMS application is internal to the IRS only. Users of the system remove any PII that would be available to those without an OL5081. The SAMS 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. 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. SAMS

User permissions are granted based on least privilege. The program contains a number of roles and users are assigned those roles based upon their function within the organization and the application.

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.

Management utilizes Business Objects Reports to monitor and evaluate user activities and to safeguard PII data within the system.

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*)? No

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? No

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.

IRS 34.037 IRS Audit Trail and Security Records System

IRS 00.003 Taxpayer Advocate Service and Customer Feedback

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:

Not Applicable