Date of Approval: 10/18/2017 PIA ID Number: **2930**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Systemic Advocacy Management System, Generation 2, SAMS II

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

NO	VISION & STRATEGY/MILESTONE 0
NO	PROJECT INITIATION/MILESTONE 1
NO	DOMAIN ARCHITECTURE/MILESTONE 2
NO	PRELIMINARY DESIGN/MILESTONE 3
NO	DETAILED DESIGN/MILESTONE 4A
NO	SYSTEM DEVELOPMENT/MILESTONE 4B
NO	SYSTEM DEPLOYMENT/MILESTONE 5
YES	OPERATIONS & MAINTENANCE (I.E., SYSTEM IS CURRENTLY OPERATIONAL)

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

A.1 General Business Purpose

5. 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 Systemic Advocacy Management System, Generation 2 (SAMS II) is a 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. Systemic advocacy program managers will develop projects from selected issues submitted. SAMS II allows the TAS Office of 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.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
Yes	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	Practitioner Tax Identification Number (PTIN)

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 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 SAMS II system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer for intergovernmental communications. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. SAMS II cannot completely eliminate the use of the SSNs and TINs. SSNs and TINs are not utilized in every issue; however, the SSN and TIN may be required to properly identify individuals where specific taxpayer information is needed to resolve the systemic issue. SSN and TIN masking is employed for outgoing letters.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

SELECTED	PII ELEMENT	ON PRIMARY	ON SPOUSE	ON DEPENDENT
YES	NAME	YES	YES	YES
YES	MAILING ADDRESS	NO	NO	NO
YES	PHONE NUMBERS	NO	NO	NO
YES	E-MAIL ADDRESS	NO	NO	NO
YES	DATE OF BIRTH	YES	YES	YES
NO	PLACE OF BIRTH	NO	NO	NO
YES	SEID	NO	NO	NO
NO	MOTHER'S MAIDEN NAME	NO	NO	NO
NO	PROTECTION PERSONAL IDENTIFICATION NUMBERS (IP PIN)	NO	NO	NO
NO	INTERNET PROTOCOL ADDRESS (IP ADDRESS)	NO	NO	NO
NO	CRIMINAL HISTORY	NO	NO	NO
NO	MEDICAL INFORMATION	NO	NO	NO
YES	CERTIFICATE OR LICENSE NUMBERS	NO	NO	NO
NO	VEHICLE IDENTIFIERS	NO	NO	NO
NO	PASSPORT NUMBER	NO	NO	NO
YES	ALIEN (A-) NUMBER	NO	NO	NO
NO	FINANCIAL ACCOUNT NUMBERS	NO	NO	NO
NO	PHOTOGRAPHIC IDENTIFIERS	NO	NO	NO
NO	BIOMETRIC IDENTIFIERS	NO	NO	NO
NO	EMPLOYMENT (HR) INFORMATION	NO	NO	NO
YES	TAX ACCOUNT INFORMATION	YES	YES	YES

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

The SAMS II application is used by TAS personnel to record, manage, process, and resolve systemic issues. SAMS II requests the individual submitting an issue through IRS.gov (public) to provide an email address for acknowledgement or possible follow-up. SSNs and TINs may be needed to properly identify individuals where specific tax account information is needed to resolve the issue. Office contact information (Name, office address, office telephone, e-mail address, and SEID) is retained for all authorized users, program contacts, and internal submitters. Additionally, names, addresses, phone numbers, and tax return information obtained to address and resolve issues will be maintained within SAMS II.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. 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. Taxpayer Advocate Service (TAS) personnel requests supporting documentation when needed. Information received is verified against IRS records and feedback is provided if information is not accurate or missing. This information either helps solve the issue, or helps identify processing problems within the IRS. Project reviews, manager reviews, and quality reviews will also identify areas of concern with data accuracy. Timeliness is ensured through contact with issue submitter.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS NUMBER	SORNS NAME
IRS 34.037	IRS AUDIT TRAIL AND SECURITY RECORDS SYSTEM
IRS 00.003	TAXPAYER ADVOCATE SERVICE AND CUSTOMER FEEDBACK

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agency(s)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

ORGANIZATION NAME	TRANSMISSION METHOD	ISA/MOU
WEB FORM ON IRS.GOV	HTTPS://WWW.IRS.GOV/ADVOCATE	NO

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

12a. Does this system disseminate SBU/PII to other IRS Systems?

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information? Individuals receive notice via the Privacy Act notice in tax return instructions. Information collected directly from the individual is voluntary. The authority and purpose for collection is explained verbally or via web form on https://www.irs.gov/advocate. Notice, consent and due process are provided pursuant to 5 USC.

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s): Individuals can verbally opt-out or refuse to respond to requests for more information. Notice, consent and due process are provided pursuant to 5 USC.

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

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	No	
Developers	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Access to the data is determined by the TAS program office. Completion of a formal request via Online-5081 containing the appropriate electronic signature and manager's approval are needed prior to receiving a system access. Additional controls include restriction of user access based on job functions and responsibilities, "need-to-know" and separation of duties. Online 5081 is used to document access requests, modifications, and terminations.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22a. 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 11/21/2016

23.1 Describe in detail the system s audit trail. 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. Outside of the SAMS application, the Wintel platform will provide additional audit trail information and will be the responsibility of systems administration. Employee login information will include who logged in, when, for how long, and what processes were run during each session. SAMS II is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. SAMS does contain privacy information, however this information cannot be accessed remotely. A Privacy and Civil Liberties Impact Assessment (PCLIA) was conducted as part of the authorization process and is updated every 3 years and as needed.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? Yes

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If **yes,** provide the date the permission was granted. 6/15/2017
If **no**, explain why not.

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees: Under 50,000
26b. Contractors: Not Applicable
26c. Members of the Public: Under 100,000
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? Yes

27a. If **yes**, explain the First Amendment information being collected and how it is used.
Information collected includes tax return income, deductions, credits, etc., that might relate to First Amendment rights (for example, charitable contributions to religious organizations). The information is used to resolve tax account problems caused by the Service's administration of the tax laws, other IRS systemic processes and policies or the tax laws themselves.

27b. If **yes**, please check all of the following exceptions (any one of which allows the maintenance of such information) that apply:

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17). Yes
The information maintained is pertinent to and within the scope of an authorized law enforcement activity. (As noted in Q 7) No
There is a statute that expressly authorizes its collection. (Identified in Q6) No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report