Date of Approval: **May 26, 2020**

PIA ID Number: **4847**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Systemic Advocacy Management System Generation 2, SAMS II

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Systemic Advocacy Management System Generation 2, SAMS II, 2930

What is the approval date of the most recent PCLIA?

10/18/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

TAS Executive Governance Board (EGB)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements

Delivery of governmental benefits, privileges, and services

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

The SSN is used because no other identifier can be used to uniquely identify a taxpayer for intergovernmental communications.

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.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Standard Employee Identifier (SEID)

Certificate or License Numbers

Alien Number

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Protected Information Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 00.003 Taxpayer Advocate Service and Customer Feedback and Survey Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

No

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

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: IRS.gov Portal
Transmission Method: manual
ISA/MOU No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

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

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

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

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.

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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Write

Managers: Read Write

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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

2/12/2020

Describe 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.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Treasury FISMA Inventory Management System (TFIMS)

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Annual Security Control Assessment (ASCA) is completed annually for SAMS II assessing one third of the control each year. When and if necessary, the required forms are submitted if live data from the SAMS II Production database will be copied to a test/development environment for testing purposes.

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

6/15/2017

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

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

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.

Please list all 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).

Will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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