Systemic Advocacy Management System II, Release 3.2 (SAMS II) – Privacy Impact Assessment

PIA Approval Date – Nov. 10, 2011

System Overview

The Systemic Advocacy Management System II, Release 3.2 (SAMS II) is a National Taxpayer Advocate Service (TAS) application and 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).

Systems of Records Notice (SORN):

- IRS 00.003--Taxpayer Advocate Service and Customer Feedback and Survey Records
- IRS 34.037--IRS Audit Trail and Security Records System

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer:
  - E–mail Address
  - Issue Subject Name
  - Issue Description in a Web Form

B. Employee:
  - SEID
  - Name
  - Office
  - Telephone Number
  - E–mail Address
  - Physical Address

C. 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

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. Taxpayer:
- E–mail Address
- Issue Subject Name
- Issue Description in a Web Form

B. Employee:
- SEID
- Name
- Office
- Telephone Number
- E–mail Address
- Physical Address

C. Other Federal Agencies – Office Contact Information:
- Name
- Office
- Telephone number
- E–mail address
- Physical address

D. State and Local Agencies – Office Contact Information:
- Name
- Office
- Telephone number
- E–mail address
- Physical address

3. Is each data item required for the business purpose of the system? Explain.
Yes. 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.

4. How will each data item 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.

5. Is there another source for the data? Explain how that source is or is not used.
SAMS II receives data from employee contact information, lightweight directory access protocol (LDAP)/Active directory for user authentication and permissions, to add a system user or to pull in

contact information. LDAP is the source of record. All other data is manually entered by SAMS II users from a roles/permission model and business rules for entry.

6. Generally, how will data be retrieved by the user?
Data is retrieved within SAMS II via the architectural pattern of Model–View–Controller (MVC). Within this pattern the view of the data is decoupled from the data in the database. The data is selected from the database via stored procedures using Microsoft's application blocks. Utilizing XML, the data file is automatically retrieved by the intranet application and saved to a database. Intranet application users have access to the issue data. Users have a Search screen within the SAMS II web application which is accessible through the IRS network. Additionally, there is a Business Objects portal that allows users to retrieve data and build reports through the Crystal Reports Builder following a permissions model.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is retrievable by:

- Submitter Name
- SEID
- E–mail address

<u>Access to the Data</u>

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Limited view access is open to anyone authorized to be on the IRS network. Additional permissions are available based on work responsibilities and/or job assignments via On–Line 5081 (OL5081). Users perform project based activities: entering Action plans, assigning tasks, contact information, notes, attaching reference materials to manage the resolution recommended for the systemic issue reported. Only the Business System Owner Administrators, and Operations Support System Administrators have access to all data, system files, and functions required to carry out their assigned tasks and responsibilities in support of the TAS business practices.

Role: Business System Owner
Permission: Access to all data, system files and functions

Role: Administrators
Permission: Access to all data, system files and functions

Role: Operations Support System Administrators
Permission: Access to all data, system files and functions

Role: Users
Permission: Perform project based activities

Role: Contractors
Permission: Access is based on work responsibilities and/or job assignments via Online 5081.

9. How is access to the data by a user 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.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes.

- Systems Providing Data to SAMS II:
  - SAMS II web form: Provides for the posting of issues submitted by external users to the internal SAMS II application (through a web form on IRS.gov). Data entered is stored to a file transport protocol (FTP) folder and imported to SAMS II via secure virtual private network (VPN).

- Systems Receiving Data from SAMS II:
  - Business Performance Management System (BPMS): Statistical data will be provided to the Business Performance management system through a limited view using the business objects report tool. No Taxpayer information. The data is fed manually to the BPMS system currently with eventual read access by BPMS reporting to compile business measure data directly. BPMS reports will draw from a TAS defined “universe” allowing access only to data elements

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes.

Business Performance Management System (BPMS)

- Security Assessment & Authorization (SA&A) – February 9, 2011, expires February 9, 2014
- Privacy Impact Assessment (PIA) – December 17, 2010, expires December 17, 2013

12. Will other agencies provide, receive, or share data in any form with this system?
No. There are no other agencies that will provide, receive or share data in any form with SAMS II. Other agencies do not have access to SAMS II. Any information collected is process related and is manually entered into SAMS II by an IRS employee.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
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 will be published under IRM 1.15.9 Records Control Schedule for Taxpayer Advocate when next updated/published.

14. Will this system use technology in a new way?
No. SAMS II will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. The information obtained via e–mail web form, etc., is not used to track back to an individual, except for communication purposes via email only, not local address. An email message may be used to send status updates to taxpayers. Statistical data about the types of issues and where they were identified (i.e., internally or externally) will be developed for trend analysis and inventory management.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No. SAMS II will not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. SAMS II does not allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not applicable. SAMS II does not make any determinations.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No. SAMS II is web–based, however, persistent cookies are not used.

View other PIAs on IRS.gov