

**System Advocacy Management System, Release II (SAMS II)
Privacy Impact Assessment**

PIA Approval Date – Feb. 20, 2009

Requested Operational Date – Target deployment date is Nov. 2008.

System Overview

The Systemic Advocacy Management System, Release II (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.

Systems of Records Notice

- Treasury/IRS 00.003 – Taxpayer Advocate Service and Customer Feedback and Survey Records
- Treasury/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:** No taxpayer data is required. Any private individual may submit issues to Taxpayer Advocate Service (TAS). Submitters on IRS.gov complete a Web-form. They are discouraged through a warning banner from entering any sensitive information beyond an optional e-mail address for subsequent contact if needed. [Actual text on warning banner: Do not submit any taxpayer or personal information, such as a Social Security number.] The form cannot prevent entry of sensitive information, but if entered it is redacted by manual review: SAMS II analyzes issues for social security number (SSN) and employee identification number (EIN) pattern of numbers. If a pattern is found, it is replaced with "Taxpayer Identification Number (TIN) Removed"; which strips the taxpayers' information. Manual review occurs within 1-2 business days, during which time the entry is visible within the IRS network. E-mail address is retained for 6 months after close of record.
- B. Employee:** System stores Standard Employee Identification (SEID). Submitters in-network may enter contact information. Internal contact information is also stored for all users who have a completed and approved On-Line 5081. Information from user tables includes: name, office, telephone numbers, e-mail address, and physical address (IP). Retention of this information facilitates contact with submitters and individuals with work assignments, as well as facilitating contact with individuals with work assignments recorded on the application.
- C. Audit Trail:** All audit trail records are identified only by SEID.
- D. Other:** None.

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

- A. IRS:** None
- B. Taxpayer:**
 - e-mail address
 - issue subject name
 - issue description in a Web form

The e-mail notifications generated to taxpayers and or other Federal Agencies that submit systemic issues do not contain any sensitive taxpayer information. They are generic notices acknowledging receipt or providing status on systemic issues only. They do not contain individual tax account information.

Since the e-mail notifications contain no SBU information, the messages are not encrypted.

C. Employee:

- the employee's SEID is captured in the authentication process.
- Office contact information:
 - name
 - office
 - telephone number
 - e-mail address
 - and physical address is retrieved from the Lightweight Directory Access Protocol (LDAP) for submitters
 - OL5081 authorized users
 - research contacts
 - and officials responsible for implementing advocacy recommendations

D. Other Federal Agencies:

- office contact information:
- name
- office
- telephone number
- e-mail address
- physical address may be recorded incidental to advocacy research if there is intersection with another agency.

E. State and Local Agencies:

- office contact information:
- name
- office
- telephone number
- e-mail address
- physical address may be recorded incidental to advocacy research if there is intersection with other agency.

F. Other third party sources:

- Submitters contribute through a Web form on IRS.gov (public IRS Website). They will enter his/her e-mail address, issue subject, and issue description in a Web form and submit. No information is retrieved from a data source other than directly entered by the practitioner, business, group, etc (per narrative Web form in which they volunteer information – same warning banner is applied as with taxpayer). The narrative is scanned and personally identifiable information (PII) is stripped.

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

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 user (e.g., employee, general public) of the system to enter accurate information

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 (See introduction for description.) This is generally recorded only for submitters within the IRS network.
- E-mail address from the contact information

Access to the Data

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 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.

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. Contractors working in connection with SAMS have no access to taxpayer SBU/PII data.

Roles and permissions

- Business System Owner Administrators, Operations Support System Administrators
Access to all data, system files and functions
- Users
Perform project based activities
- Contractors
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.

10. Do other IRS systems provide, receive, or share data in the system?

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). Performance data will be provided to the Business Performance management system through the business objects report tool.

Systems Receiving Data from SAMS II

- Business Performance Management System (BPMS): 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 necessary for business measures.

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

IRS.gov:

- Certification & Accreditation (C&A) – December 19, 2007, expires December 12, 2010
- Privacy Impact Analysis (PIA) – September 2006, expires September 2009
- MITS public user portal has responsibility for access control.

SAMS:

- C&A – June 18, 2008, expires June 18, 2010
- PIA – June 7, 2007, expires June 7, 2010

BPMS:

- C&A – February 19, 2008, expires February 19, 2011
- PIA – June 19, 2007, expires June 19, 2010

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.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

The data in the system is permanently archived not eliminated. No process has been defined to dispose of records. Records management is included in a future TAS system enhancement. TAS will work on defining a process to define disposal of records.

The SAMS database will be archived in accordance with Federal Records Retention Standards for electronic information.
Data is eliminated via IRM 1.15.9.11 – Records Control Schedule for the taxpayer advocate service. Retention time frames have currently not been exceeded for any system data.

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?

No. The information obtained via e-mail Web form, etc., is not used to track back to an individual, except for communication purposes. An e-mail 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?

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](#)