Specific & Spontaneous Exchange of Information (S&SEI) - Privacy Impact Assessment

PIA Approval Date - May 12, 2006

Requested Operational Date - Currently Operational

System Overview

The Specific & Spontaneous Exchange of Information Program Tracking System (S&SEI) tracks the Routine Exchange of Information between the United States and other foreign competent authorities. The database contains the date of the request, the name of the requesting official, the name of the taxpayer being requested and other inventory control measures.

Systems of Records Notice (SORN)

- Treasury/IRS 49.001 Collateral and Information Requests System
- 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:**
   S&SEI tracks the exchange of information requests between the United States and other countries. The database contains the date of the request, name of country, the name of the taxpayer being requested and other inventory control measures.

   A. Taxpayer: The following information is available:
   - case number;
   - suffix;
   - case name;
   - taxpayer name;
   - category;
   - expedite feature;
   - region/Business Operating Division (BOD);
   - action office;
   - country;
   - supplemental request;
   - information types (i.e., codes to retrieve bank account information, credit card, and tax shelter information); and
   - summons required (yes/no field).

   B. Employee: The employee's user ID (Standard Employee Identification Number [SEID]) is obtained from the Windows NT LAN Manager (NTLM) authentication to control access to the application.

   - IRS employee name;
   - Revenue Service Representative (RSR) post;
   - date (i.e. assigned, request initiated, request received, case closure)
   - status of case;
   - information secured;
   - appreciation memo (yes/ no field);
   - appraisal questionnaire (yes/no field); and
   - comments.

C. Audit Trail Information: Auditing is only performed at the General Support System (GSS) level. MITS-14 GSS (Washington, D.C. Territory and New Carrollton Territory) auditing captures user workstation and log on/off activities. It also logs system administrator and security administrator activities. The audit logs have critical event information (type of event, source of event, time and date of event, user accountable for event) that is useful for identifying system intrusion detection and system forensics should an attack occur. Logs are regularly reviewed.

System administrators and security administrators' actions are recorded while logged onto the system in their respective administrator role or their user mode. Audit records are created and maintained such that they are protected from modification, tampering, unauthorized access, or destruction. Any user cannot modify audited events once the event has occurred. All modifications to the events being collected are audited and detected.

D. Other: None

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

   A. IRS: S&SEI does not communicate with other IRS systems, internal or external. Information received from the exchange of information requests made pursuant to treaties between the US and other countries is manually entered into the system.

   B. Taxpayer: None

   C. Employee: None

   D. Other Federal Agencies: None

   E. State and Local Agencies: None

   F. Other third party sources: None

3. **Is each data item required for the business purpose of the system? Explain.**
   Yes. S&SEI tracks the exchange of information requests between the United States and other countries and the data collected is for the processing and administrative management of these requests.

4. **How will each data item be verified for accuracy, timeliness, and completeness?**
   S&SEI limits user inputs for designated fields within the application. The valid syntax of application inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. In addition, the application checks for completeness and validity of entered data items.

5. **Is there another source for the data? Explain how that source is or is not used.**
   No. There are no other sources of information.

6. **Generally, how will data be retrieved by the user?**
   Users use a search function based on key data fields to retrieve information (e.g., case number, case name).

7. **Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?**
   No. Data is retrieved by case number, case name, or country.

Access to the Data

8. **Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?**
   The following are user roles for S&SEI:
   - Admin - has the capabilities to delete, update, close, and add a request.
   - Manager - provides users with the capabilities to add, update, and close a request.
   - Analyst - has the capabilities to update and close a request.

   There are eleven (11) regular users and fifteen (15) users elevated privileges totaling 26 users around the world that have access to the S&SEI application.

   No contractors will have access to the S&SEI system.

9. **How is access to the data by a user determined and by whom?**
   Access is authorized by a LMSB manager.

   The S&SEI application relies on the GSS for user identification and authentication (login and password) mechanism. Users are identified uniquely by the SEID from their IRS LAN domain credentials. A user with IRS LAN domain credentials can only obtain access to the application if the user has been assigned a role within the S&SEI SQL Server (provided by the database administrator) and the user has the client-side module installed on their workstation.

   To request access to S&SEI all personnel must submit a request to the application POC. Users are uniquely identified by their SEID. Once the requests have been approved by the user's manager, the requests are automatically routed to the S&SEI application POC for approval. Then the user is provided access via the database administrator.

   S&SEI utilized three types of Active Server Page (ASP) forms as an access enforcement mechanism. This mechanism is employed by LMSB to control access between the user and the fields within the database.

   The following are the three (3) different forms used to enforce access—
   - Admin - provides users with the capabilities to delete, update, close, and add a request.
   - Manager - provides users with the capabilities to add, update, and close a request.
   - Analyst - provides users with the capabilities to update and close a request.

   The ASP Form utilized by the S&SEI application enforces the most restrictive set of right/privileges or access needed by users to perform their tasks, thereby enforcing least privilege. Users are only granted access to roles that are necessary to perform the tasks associated with their job.

10. **Do other IRS systems provide, receive, or share data in the system?**
    No. S&SEI does not communicate with other IRS systems, internal or external. Information received from the information requests made pursuant to treaties between the United States and other countries is manually entered into the system.

11. **Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?**
    Not applicable.

12. **Will other agencies provide, receive, or share data in any form with this system?**
    No (i.e., for data directly shared with S&SEI).

    Formal Exchange Agreements are held with tax authorities of other nations that, in part, authorize information sharing as is directly related to the business purpose of the system. It should be noted that data itself is not directly processed to/from S&SEI; hence, data exchange or interconnection agreements are not applicable. The “Formal Exchange Agreement” is a high level agreement necessary to create a formal understanding to carry out operations/requests with other countries.

Administrative Controls of Data

13. **What are the procedures for eliminating the data at the end of the retention period?**
    Data is held indefinitely and is, therefore, not eliminated from the system. An IRM reference supporting this approach could not be provided.

14. **Will this system use technology in a new way?**
    No. This system will not use technology in a new way.

15. **Will this system be used to identify or locate individuals or groups?**
    No. S&SEI tracks the exchange of information requests between the United States and other countries and cannot be used to identify or locate individuals or groups.

16. **Will this system provide the capability to monitor individuals or groups?**
    No. S&SEI tracks the exchange of information requests between the United States and other countries and cannot be used monitor individuals or groups.

17. **Can use of the system allow IRS to treat taxpayers, employees, or others, differently?**
    No. The system cannot be used to treat taxpayers or employees disparately and the information cannot be used to make determinations that will result in a negative action against a taxpayer.

18. **Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?**
    N/A. S&SEI tracks the exchange of information requests between the United States and other countries. It does not make determinations that will result in a negative action which would necessitate due process procedures.

19. **If the system is Web-based, does it use persistent cookies or other tracking devices to identify Web visitors?**
    No. S&SEI is not a Web-based system.

View other PIAs on IRS.gov