Taxpayer Advocate Management Information System (TAMIS)
Privacy Impact Assessment

PIA Approval Date - July 30, 2008

System Overview
The Taxpayer Advocate Management Information System (TAMIS) provides case inventory control and case activity recordation for the Taxpayer Advocate Service (TAS) caseworker. TAMIS also provides statistical analysis and reporting for TAS management and third parties with oversight authority. GUI-TAMIS stands for the version of this application designed to operate in an MS-Windows environment and utilizing a windows-like interface while providing access to a centralized, mini-computer-based database.

I. Data in the System

The Taxpayer Advocate Management Information System (TAMIS) provides case inventory control and case activity recordation for the Taxpayer Advocate Service (TAS) caseworker. TAMIS also provides statistical analysis and reporting for TAS management and third parties with oversight authority. GUI-TAMIS stands for the version of this application designed to operate in an MS-Windows environment and utilizing a windows-like interface while providing access to a centralized, mini-computer-based database.

1. Generally describe the information to be used in the system in each of the following categories:

- Taxpayer:
  Taxpayer name, Taxpayer Identification Number, address, Power of Attorney name, primary & secondary telephones, best time to contact, fax number.
- Employee:
  Employee number and organization code, level of access and login name, employee name, title, address, city and state, local phone, toll- free phone and fax number, hours and days available and time zone.
- Audit Trail Information (including employee log-in info):
  Within the TAMIS application two tables provide most of the audit trail information. The audit log table records actions taken (user action), who performed the action (user_emp_id), on what case the action was taken (case no., or emp id if the action was to the employee table), and when the action was taken (date stamp).
  The audit changes table records the before and after values of any changed field; the audit seq joins the audit changes table to the master record in the audit log table.
  Additional audit_<table name> tables hold copies of records from their counterpart tables when a record is deleted.
  Outside of the TAMIS application, the Sun platform will provide additional audit trail information and will be the responsibility of systems administration there. Employee login information will include who logged, when, for how long, and what processes were run during each session.
- Other:
  Various management information data relating to Taxpayer Advocate Service cases including case file number (systemically generated), ATAO/TAO code, subcode and relief date, received and closed dates, re-opened indicators by number of times and reason, organization codes, problem description, major issue codes, business operating

division code, customer satisfaction and ICP codes, and project tracking, local use and case complexity codes.

2. What are the sources of the information in the system?

Case referrals from IRS Campuses and local offices and/or direct communication with the Taxpayer Advocate Service by taxpayers, or their representatives, through the telephone, mail, e-mail, or walk-in/face-to-face contacts and completion of Form 911, Request for Taxpayer Assistance Order, or from the Desktop Integration (DI) system.

Taxpayers or individuals who initiate correspondence on behalf of a taxpayer such as a power of attorney and other third parties, including financial institutions, suppliers and other vendors, as required to resolve the taxpayer's case.

a. **What IRS files and databases are used?**
The TAMIS system is an Oracle Relational database that resides on a SUN 25k platform in the Detroit Computing Center. TAMIS gets cases from the Desktop Integration (DI) system which also uses an Oracle Relational database. Entity data is available through IDRS. Data relating to specific case actions is not retrievable elsewhere.

b. **What Federal Agencies are providing data for use in the system?**
No Federal Agencies provide data for use in TAMIS.

c. **What State and Local Agencies are providing data for use in the system?**
No State or Local Agencies provide data for use in TAMIS.

d. **From what other third party sources will data be collected?**
Taxpayers or individuals who initiate correspondence on behalf of a taxpayer such as a power of attorney and other third parties, including financial institutions, suppliers and other vendors, as required to resolve the taxpayer's case.

e. **What information will be collected from the taxpayer/employee?**
Taxpayer name, social security number, address, POA name, primary and secondary telephone, best time to contact, fax number.

3. a. How will data collected from sources other than IRS records and the taxpayers be verified for accuracy?

The Taxpayer Advocate caseworker is in contact with the taxpayer or the taxpayer representative and requests supporting documentation for the case then verifies information received with what IRS systems show for the taxpayer.

b. **How will data be checked for completeness?**

The taxpayer will provide feedback if the information is not accurate or missing since the proposed resolution of the case will not be acceptable. Caseworker reviews, managerial reviews, and quality reviews will also identify areas of concern.

TAS case workers verify data received from the taxpayer or the taxpayer representative against the records IRS has for that taxpayer. This data either helps solve the taxpayer's problem, helps determine if the problem is the taxpayer's or the IRS's fault, or helps identify processing problems within the IRS.

c. Is the data current? How do you know?

Taxpayer Advocate case workers verify the information received from all sources against IRS records and enters the most current information into the TAMIS system.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

Data elements for TAMIS are described in the TAMIS FSP, Data Dictionary, Section 5, Data Elements. The data tables for TAMIS are described in Section 4, Data Stores (Entities).

II. Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

Associate Advocates, Senior Associate Advocates, Group Managers, Program Analysts and Taxpayer Advocates and their support staff at the local, area and national levels, and IRS personnel in other, related, business units with a business need-to-know such as the Problem Solving Day Coordinator or various Operating Division liaison staff who handle the transfer of cases between their division and TAS.

Those cases on TAMIS that are assigned to TAS employees will only be accessible to TAS employees or W&I/SBSE employees working the (NTA) National Toll-Free telephone number. All other cases in the TAMIS database not assigned to TAS employees will be accessible by all TAMIS users.

All IRS personnel who have access to TAMIS have filled out Form 5081 and are only granted access when their jobs require it. Their access is immediately revoked when it is no longer required.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to the data within the system is restricted. Users are restricted to only those pieces of the system to which they need access.

IRS personnel are required to complete Form 5081, Information System User Registration/Change Request, containing the necessary authorizing signature of the user's manager, prior to receiving a system account or TAMIS database account. Data access on the system is restricted to users who have a need-to-know and/or process Taxpayer Advocate cases and through the use of permission levels in both the operating system and the TAMIS database. In addition, data modification is restricted by use of permission levels, user job function and need-to-know criteria.

A user's position and need-to-know determines the level of access to the data. The System Administrator grants approval for system access. A user's access to the data terminates when the user no longer requires access to TAMIS. Criteria, procedures, controls, and responsibilities regarding access are documented in the TAMIS Security Features User's Guide.

Access to TAMIS is accomplished through the I&A functions contained within the Oracle operating system on the 25K platform that require all users to identify themselves and provide proof of their identities by user identification (USERIDs) and authentication (passwords). USERIDs and passwords are unique to each user.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

A user's position and need-to-know determines the level of access to the data. The System Administrator grants approval for system access. A user's access to the data terminates when the user no longer requires access to TAMIS. The criteria, procedures, controls and responsibilities regarding access are documented in the TAMIS Security Features User's Guide.

The program contains a number of access levels for users based upon their necessary function within the organization.

Users with an access level of 0 are query/view only.

Users with an access level of 1 are limited case workers and can only query/view cases and edit cases assigned within their org code.

Users with an access level of 2 are considered full case workers and have the ability to query/view, add, and edit cases assigned to them or cases within their org code.

Users with an access level of 3 are TAS Managers, they have full access to cases and can update employee records belonging only to their own assigned org code.

Users with an access level of 4 are TA & TA Staff, they can update employee records belonging only to their own assigned organization code

Users with access level of 5 can update employee records belonging to any organization code. Level Full Access allows a user to add/update information as it necessary and to compose letters and generate reports/listings.

The TAMIS Risk Assessment (RA), February 5, 2002, determined that the minimum-security class of C2 (Controlled Access Protection) is required for TAMIS, and satisfies the review and configuration management requirements. The TAMIS system requires all users to have the appropriate clearances or authorization, however all users do not have the same need-to-know or access for all the information within the system. Treasury and IRS directives require systems that contain Sensitive But Unclassified (SBU) information to attain C2 security functionality.

TAMIS stores information protected under the Privacy Act of 1974. Such information is categorized as SBU. In addition, the Commissioner of the IRS has designated that all IRS systems and associated data be categorized as SBU, and protected under IRC 6103, Confidentiality and Disclosure of Return and Return Information.

Risk Assessments have been performed in accordance with the following guidelines:
1. IRM 2.1.10, Information Systems Security, April 30, 1998.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

TAMIS uses audit trails as required by IRS 2.1.10, Information Systems Security, May 1998, and a Functional Security Coordinator is assigned. All employees are required to attend UNAX Training and they have been trained on the use of the system and their responsibilities concerning access and use of the data.

The following mandatory rules are defined for users of IRS computer and information systems:

- Users are forbidden to access, research, or change any account, file, record, or application that is not required to perform official duties.
- Users are restricted to accessing, researching, or changing only accounts, files, records, or applications that are required to perform their official duties.
- Users are restricted from accessing their individual/spouse account, accounts of relatives, friends, neighbors, or any account in which the user has a personal or financial interest. Users are restricted from accessing the accounts of a famous or public person unless given authorization to do so.
- If asked to access an account or other sensitive or private information, users are required to verify that the request is authorized and valid. Users will be held accountable if they access an unauthorized account.

5.a. Do other systems share data or have access to data in this system? If yes, explain.

The Taxpayer Identification Number (TIN) will cause the taxpayer's name and address to autopop from IDRS, subject to updating at time of input. The Desktop Integration (DI) system adds cases to TAMIS but does not retrieve information back from TAMIS. Business Performance Management System (BPMS) will access data posted to a separate statistical database within TAMIS which will provide counts of cases, but not actual taxpayer data. BPMS will extract this data on a regular basis to generate the reports they need.

b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?

The Director, Detroit Computing Center (DCC) is responsible for protecting the privacy rights of taxpayers and employees regarding data contained within TAMIS.

6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

Major issue code and hardship code data are shared with Congress, as directed by law (26 USC 7803(c)(2)(B)); and with TIGTA/GAO, pursuant to official notification and in compliance with RRA '98 entitling TIGTA access to all IRS data for purposes of periodic audits. Headquarters Research for research studies and to assist TAS in providing better customer service.

b. How will the data be used by the agency?

By law Congress requires an annual report from Taxpayer Advocate Service to support their mission to "help taxpayers solve problems with the IRS and recommend changes that will prevent them." TIGTA requests data annually for auditing purposes to ensure UNAX and 1203 RRA '98 rules are upheld for any TAMIS user accessing the system.

c. Who is responsible for assuring proper use of the data?

TAMIS System Administrators and Information Technology Specialist follows procedures set forth by law and RRA '98 in providing the requested information to the TAS organization for Congress and to TIGTA. No other agency has direct assess to the TAMIS system data.

d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?

Treasury Inspector General for Tax Administration (TIGTA) requests an annual download for auditing purposes but does not access the system directly. Information within the system will not be disclosed except as expressly authorized by IRC 6103.

III. Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. The data used in TAMIS is both relevant and necessary to the purpose for which the system has been designed.

2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

TAMIS does not derive or create previously unavailable data about an individual through aggregation from the information collected.

b. Will the new data be placed in the individual's record (taxpayer or employee)?

TAMIS does not derive or create previously unavailable data about an individual through aggregation from the information collected.

c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?

TAMIS cannot make determinations about taxpayers or employees.

d. How will the new data be verified for relevance and accuracy?

TAMIS does not derive or create previously unavailable data about an individual through aggregation from the information collected.

3.a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

TAMIS data is not being consolidated. Existing security controls will remain in place, which restrict users to only inputting and updating data within their organization code.

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain

The proper security controls will remain in place restricting users to inputting and updating only the data within their organization code. UNAX Training will also be provided to each user.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

Files can be retrieved by taxpayer name, SSN, or by case number.

What are the potential effects on the due process rights of taxpayers and employees of:

a. consolidation and linkage of files and systems;

TAMIS does not consolidate processes or link files

b. derivation of data;

TAMIS does not derive data.

c. accelerated information processing and decision making;

The accelerated information processing performed by the TAMIS system does not affect the due process rights of the taxpayers or employees.

TAMIS does not perform any decision-making.

d. use of new technologies;

The TAMIS configuration is not new technology. TAMIS did just convert to an Oracle 10g database and is housed on a Sun 25K server Detroit Computing Center. There are no new technologies implemented with this system.

How are the effects to be mitigated?

TAMIS does not link files, connect with other systems, derive data, provide decision-making capability, or use new technologies. TAMIS does not affect the due process rights of taxpayers or employees.

IV. Maintenance of Administrative Controls

1.a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.

The TAMIS System allows for inventory control, data analysis, automated internal transaction processing, and automated standardized letter/form processing.

System management is responsible for the proper operation of the system, ensuring correct processing and responses to users, as well as the oversight of employees' use of the system and the data contained therein.

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

TAMIS is housed at the DCC. TAMIS production takes place on the Sun 25K server via web access from a standard IRS workstation. The TAMIS application resides on a Sun 25K providing an interface to the database allowing users to input, research and update records. All TAMIS data is processed and stored on the Sun25K server.

c. Explain any possibility of disparate treatment of individuals or groups.

TAMIS does not provide any facility to provide special treatment for any taxpayer or employee. Its purpose is to identify situations where a taxpayer or taxpayers are being treated differently than allowed by laws or regulation and to correct those situations.

2.a. What are the retention periods of data in this system?

The active database contains records for the current and prior fiscal years. The archived or inactive database contains closed case records for the two preceding fiscal years. Data older than this is stored to tape.

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

The procedure for archiving TAMIS case data consists of the TAMIS System Administrator at the Detroit Computing Center (DCC) executing an archive script from a shell prompt. These procedures are documented in the Taxpayer Advocate Management Information System (TAMIS) SYSTEM ADMINISTRATOR GUIDE, Version 4.0.

When the retention period expires for data stored on tape, the tape will be demagnetized and put back in circulation for reuse. These procedures are outlined in the TAMIS Application System Security Plan.

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

The taxpayer will provide feedback if the information is not accurate since the proposed resolution of the case will not be acceptable. Caseworker reviews, managerial reviews, and quality reviews will also identify areas of concern.

3.a. Is the system using technologies in ways that the IRS has not previously employed (e.g., Caller-ID)?
TAMIS is not using technologies in ways that the IRS has not previously employed.

b. How does the use of this technology affect taxpayer/employee privacy?
TAMIS is not using technologies in ways that the IRS has not previously employed.

4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
Yes. Information included in TAMIS cases contains individual taxpayer information such as name, address, and taxpayer identification number.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.
Yes. Information contained in TAMIS cases contains individual taxpayer information such as name, address, and taxpayer identification number.

c. What controls will be used to prevent unauthorized monitoring?
Only authorized employees have access to the information on TAMIS. All employees and contractors receive UNAX and Code of Conduct training. Identification and access provisions are employed.

5.a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

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

b. If the system is being modified, will the SOR require amendment or revision? Explain.
No revision is required.

View other PIAs on IRS.gov