Treasury Inspector General for Tax Administration (TIGTA) Privacy Impact Assessment (PIA)

Name of System: TIGTA Enterprise System (TES)

Date of Submission: 6/15/2007

Contact:
Damon Plummer, Deputy Assistant Inspector General/CIO, OIT, 202-927-7163,
damon.plummer@tigta.treas.gov

Keith Kratzer, Chief Technology Officer, OIT, 770-452-4001,
keith.kratzer@tigta.treas.gov

1. What is the purpose of the system?
The Treasury Inspector General for Tax Administration (TIGTA) Enterprise System (TES) is the system infrastructure which provides data access and the computing services for TIGTA's Audit and Investigations business functions and allows them to perform their mission.   TES promotes productivity and efficiency by giving the users access to automated tools that are utilized in the performance of duties. The system consists of data extracts from various electronic systems maintained by governmental agencies and other entities.   The data is used for audit and investigative purposes and is necessary to identify and prevent fraud, waste, and abuse in the programs and operations of the Internal Revenue Service (IRS) and related entities as well as to promote economy, efficiency, and integrity in the administration of the Internal Revenue laws and deter wrongdoing by IRS and TIGTA employees or contractors.

2. What legal authority authorizes the purchase or development of this system?
The nature and scope of TIGTA's oversight and investigative responsibilities are established and set forth in the Inspector General Act of 1978, 5 U.S.C Appendix 3 and Treasury Order 115-01.   In order to enable TIGTA to perform its oversight and investigative functions, the Inspector General Act of 1978 authorizes TIGTA to have access to "all record, reports, audits, reviews, documents, papers, recommendations, or other material" maintained by the IRS. In addition, both the Privacy Act and I.R.C §6103(h)(1) authorizes TIGTA to receive information for purposes of performing its official responsibilities.

3. Under which Privacy Act SORN does the system operate?
TIGTA published its systems of records notices in the Federal Register. The Office of Investigations system of records was published at 70 F.R. 71189 (November 25, 2005) and the remainder of TIGTA's systems of records was published at 70 F.R. 46288 (August 9, 2005).

Treasury/DO .301-TIGTA--General Personnel and Payroll,
Treasury/DO .302-TIGTA--Medical Records,
Treasury/DO .303-TIGTA--General Correspondence,
Treasury/DO .304-TIGTA--General Training,
Treasury/DO .305-TIGTA--Personal Property Management Records,
Treasury/DO .306-TIGTA--Recruiting and Placement Records,
Treasury/DO .307-TIGTA--Employee Relations Matters, Appeals, Grievances, and
Complaint Files,
Treasury/DO .308-TIGTA--Data Extracts,
Treasury/DO .309-TIGTA--Chief Counsel Case Files,
Treasury/DO .310-TIGTA--Chief Counsel Disclosure Section,
Treasury/DO .311-TIGTA--Office of Investigations Files.

4. What categories of individuals are covered by the data in the system?
- Individuals who have filed, are required to file tax returns, or are included on tax returns, forms, or other information filings.
- Entities who have filed or are required to file tax returns, IRS forms, or information filings as well as any individuals listed on the returns, forms and filings; and
- Taxpayer representatives
- The subjects or potential subjects of investigations
- The subjects of complaints received by TIGTA
- Persons who have filed complaints with TIGTA
- Confidential informants
- Current and former employees or contractors of TIGTA and the IRS
- Freedom Of Information Act (FOIA) requestors

5. What are the sources of information in the system?
The Internal Revenue systems of records listed in the Computer Matching Agreement between TIGTA and the IRS are the main source of data used in the TES system. When audits or investigations warrant additional information may be received from other federal agencies such as Department of Treasury, Department of Justice, Federal Bureau of Investigations. The TES system maintains a wide variety of data and information. This includes but is not limited to the following:

- Personal data includes personnel data for TIGTA employees and personal data for private citizens.

- Financial data includes Departmental financial data and financial data for private citizens

- Investigation data includes both current and historical investigation data and information

- Workflow data includes data and information about current, past and future work processes and procedures

TIGTA does not routinely receive any data from state and local agencies, or third party sources.   TIGTA may receive such information in the course of performing an audit or investigation, but the data collected will only be used within the limited scope of the audit or investigation**.**   As necessary, auditors may contact taxpayers directly to obtain information relevant to the taxpayers' tax filing history or tax account balances. Auditors may also obtain taxpayer feedback data relevant to the taxpayers' dealings with IRS taxpayer assistance facilities.   Some information is gathered during the course of TIGTA investigations by collecting information from persons acquainted with the individual under investigation, third party witnesses, or confidential informants.

6. How is the data in the system verified for accuracy, timeliness, and reliability?
The accuracy of the data is generally contingent upon the correctness of the information provided by the IRS or TIGTA employees with respect to personnel data or by the taxpayers with respect to tax account data.   The accuracy of any finding provided by the data will be verified during the course of any investigation or audit.   TIGTA will take appropriate steps to independently verify information produced through the use of independent inquiry to resolve any discrepancies or inconsistencies with the source data provided.

TIGTA guidelines provide procedures that should be performed by the TIGTA auditors to satisfy the requirements regarding the reliability of computer-processed data.   The Government Accountability Office's (GAO) Government Auditing Standards (GAS) provide standards and requirements for financial and performance audits to include assessment of the reliability of computer-processed data.   In addition, the GAO guide, Assessing the Reliability of Computer-Processed Data (GAO-03-273G), dated October 2002, provides a conceptual framework and requirements for determining the validity and reliability of data from computer-based systems and detailed definitions.   Audit teams assess data reliability when it is used to support audit findings, conclusions, or recommendations.   The results and basis for assessing the reliability of computer-processed data is documented in the work papers and the audit report.

TIGTA guidelines provides instruction on the data to be captured for complaints and investigations to properly document, account for, and track all complaints referred to TIGTA from external sources. TIGTA employees are responsible for entering all relevant complaint and investigation data in an accurate, complete and timely manner. TIGTA employees are responsible for reviewing the data and validating the completeness and accuracy of data entered.

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

TES is the system infrastructure that TIGTA employees use to perform their day-to-day duties.   The information is used by TIGTA for audit and investigative purposes and is necessary to identify and prevent fraud, waste, and abuse in the programs and operations

of the IRS and related entities as well as to promote economy, efficiency, and integrity in the administration of the internal revenue laws and detect and deter wrongdoing by IRS and TIGTA employees.   The specific data elements that will be used vary depending on the unique needs of each audit or investigation.

8. What are the retention periods and the procedures for disposition of the data in the system?
Some of the records in this system are maintained and disposed of in accordance with a record disposition schedule approved by the National Archives and Records Administration (NARA).   TIGTA is in the process of requesting approval of new records schedules concerning all records in this system of records. Records not currently covered by an approved record retention schedule will not be destroyed until TIGTA receives approval from NARA.

9. Will this system provide the capability to identify, locate, and monitor individuals?
The use of data stored in TES allows auditors and investigators to perform comprehensive analyses of employee, taxpayer, and tax administration data in order to prevent and detect fraud and abuse in the programs and operations of the IRS and related entities.   TIGTA's computer matching program involves proactive efforts to detect fraud and prevent misuses of IRS computer data, systems, and operations. This program utilizes computer matches to create models to identify alleged misconduct and criminal violations.

10. What controls will be used to prevent unauthorized monitoring?
TIGTA Rules of Behavior state "Do not access, research, or change any account, file, record, or application not required in performing your official duties".   TIGTA employees should always verify that the request of accessing data has been authorized. All TIGTA employees are required to undergo yearly security, privacy and ethics training.   System access is monitored closely and if a user or an administrator violates the organization's security policies is subject to disciplinary action, up to and including termination of employment. TES users, administrators, and helpdesk personnel protect TIGTA from unwanted access and are on the front line in the organization's ability to respond to incidents.

The Computer Matching Agreement between TIGTA and IRS sets forth the terms under which TIGTA will match IRS computerized data to detect fraud, waste, and abuse concerning activities of the IRS as well as to identify IRS current and former employees or contractors who have violated, laws, rules or regulations and protect against attempts to corrupt or threaten the IRS or its employees.

11. Who will have access to the data in the system and what controls are in place to prevent misuse?
TES is an internal system that is not accessible by the public. The TES system contains sensitive data that needs to be protected and guarded to the maximum extent possible. Everyone who has been granted access to the system is responsible for providing the level of protection warranted by the classification of the information and material in his or her possession or control.

The Privacy Officer, System Owners, Managers and everyone in TIGTA who has access to the data are responsible for assuring the proper use of the data. System access for users, developers, and administrators accounts will be restricted to the functionality needed by the employee to perform his or her job. For data files that are deemed sensitive for general access additional preventative controls have been built into applications to provide additional restrictions to user access.