Financial Management Service

Privacy Impact Assessment

The Financial Management Service (FMS) Mission is to provide central payment services to Federal Program Agencies, operate the federal government's collections and deposit systems, provide government-wide accounting and reporting services, and manage the collection of delinquent debt owed to the government.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html

Document Date: **December 2, 2011**

Document Version: **1.0**

Name of System: **Transaction Reporting System (TRS)**

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

TRS is an FMS-wide transaction broker, data warehouse and reporting solution that provides TRS and its trading partners with a single touch point for the exchange of all financial transaction information across all FMS collections systems. This enables FMS to normalize financial transaction reporting and standardize the availability of funds and financial information across all settlement mechanisms and collection systems. TRS greatly improves transaction information reporting which eliminates redundancies and disconnects across and between the numerous point-to-point connections currently in-place between collection agents and Federal agencies.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

Treasury/FMS.017 – Revenue Collection Records

3) If the system is being modified, will the SORN require amendment or revision?
__yes, explain.
_X_no

4) Does this system contain any personal information about individuals?
_X_yes
__no

a. Is the information about members of the public?

Potentially. Sending Trading Partners ("STPs") can send TRS individually identifiable information about a member of the public.

b. Is the information about employees or contractors?

Potentially. An STP could send TRS individually identifiable information about an employee or contractor, but only as the individual is a member of the public.

5) What legal authority authorizes the purchase or development of this system?

The Secretary of the Treasury has authority to designate financial institutions as depositaries and financial agents of the United States to perform essential banking

services pursuant to 12 United States Code (USC) 90 and 265, 31 USC 3303, and other authorities.

The Secretary of the Treasury has delegated to FMS the authority to select and designate depositaries and financial agents for, among other purposes, providing TRS and related services.

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   __ Employees
   __ Contractors
   __ Taxpayers
   _X_ Others (describe)

   Individuals and organizations that make payments to Federal government agencies, and user profile information of system users.

2) **Identify the sources of information in the system**
   Check all that apply:
   __ Employee
   __ Public
   __ Federal agencies
   __ State and local agencies
   _X_ Third party

   a. **What information will be collected from employees or contractors?**

      None

   b. **What information will be collected from the public?**

      None

   c. **What Federal agencies are providing data for use in the system?**

      None

   d. **What State and local agencies are providing data for use in the system?**

      None

   e. **From what other third party sources will data be collected?**

      STPs are the source of information in TRS. STPs are entities that provide government information to TRS.

3) **Accuracy, Timeliness, and Reliability**

   a. **How will data collected from sources, other than FMS records, be verified for accuracy?**

      STPs verify the accuracy of all data collected from sources other than FMS records before transmitting data to TRS.

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

      STPs verify the completeness of all data before the data is sent to TRS.

   c. **What steps or procedures are taken to ensure the data is current?**

      Data currency is determined by the STP.

   d. **In what document(s) are the data elements described in detail?**

      Data elements that are sent to TRS by the STP are documented in the Interface Specification document that is created for each STP.

ATTRIBUTES OF THE DATA:

1) **How is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

   All of the data collected by TRS is relevant and necessary for the system purpose described in the System Overview above.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?**

   No

3) **Will the new data be placed in the individual's record?**

   N/A

4) **Can the system make determinations about employees or members of the public that would not be possible without the new data?**

   N/A

5) **How will the new data be verified for relevance and accuracy?**

   N/A

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

TRS has flexible access control through the use of data type and data value data permissions that protect data from unauthorized access or use.

Every user is a member of an access group and is limited to the roles, files, and trading partner data in that access group.

TRS data access control is implemented in compliance with the FMS information security requirements of *separation of duties* and *least privilege*.

TRS follows all NIST, Treasury, and FMS security policies, procedures, and standards for access control.

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

Processes are not consolidated.

8) **How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)**

Data is retrieved based on the information provided by the STPs. Data is not retrievable by personal identifiers.

9) **What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

No reports can be produced on individuals.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)? How can individuals grant consent?**

TRS does not work directly with individuals. Each STP has the opportunity to decline to send information to TRS.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **What are the retention periods of data in this system? How long will the reports produced be kept?**

Data is retained up to 1 year for transmission files from the STP depending on the retention parameter in the file profile. Reports are kept as long as the user is logged into TRS, however, the user can reproduce the report as long as the data is maintained in TRS which is currently 7 years.

2) **What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?**

No records are destroyed unless authorized under National Archives and Records Administration (NARA)-approved retention schedules and approved for destruction, in writing, by FMS Chief Counsel.

Disposition procedures are documented in the TRS Record Retention Policy.

3) **If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?**

TRS is operated in only 1 site.

4) **Is the system using technologies in ways that FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

5) **How does the use of this technology affect employee or public privacy?**

N/A

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

No

7) **What kind of information is collected as a function of the monitoring of individuals?**

N/A

8) **What controls will be used to prevent unauthorized monitoring?**

N/A

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
Check all that apply:

__ Contractors
_X_ Users
_X_ Managers
_X_ System Administrators
_X_ System Developers
__ Others (explain)_____

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

User access is based on access group, role, file, and trading partner profile data permissions on User Setup Worksheets signed by Access Group Managers. Users can also be restricted from accessing PII data. Standard Operating Procedures (SOPs) are developed, maintained, and used by the TRS Call Center.

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

A user's access is restricted by the access group, role(s), function(s) and data permissions based on their business need specified on their User Setup Worksheet. Access can be further restricted to exclude PII data.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

Software is in place to control access to data in the system. Before gaining system access, and annually thereafter, all users are required to read and agree to the TRS Rules of Behavior.

5) **If contractors are/will be involved with the design, development or maintenance of the system were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?**

Yes

6) **Do other systems share data or have access to the data in the system?**
_X_yes
__no

If yes,

a. Explain the interface.

All interfaces are with systems authorized and explained in the TRS System Security Plan (SSP).

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

For each STB boarding this role is shared by the sub-project implementation team, TRS Security Officer, TRS ISSO, and TRS Project Manager to ensure parties involved in TRS interfaces comply with FMS policies that protect the privacy rights of the affected public and employees.

7) Will other agencies share data or have access to the data in this system?

_X_yes
__no

If yes,

a. Check all that apply:

_X_Federal
__State
__ Local
__Other (explain) _____

b. Explain how the data will be used by the other agencies.

The other agencies will use TRS data for collections analysis and data reporting.

c. Identify the role responsible for assuring proper use of the data.

The TRS System Owner is responsible for assuring proper use of the data.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html