



The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service Privacy - FMS Impact Assessments (PIA): <http://www.fms.treas.gov/pia.html>

Fiscal Service Privacy – Public Debt Impact Assessments
(PIA): http://www.treasurydirect.gov/privacy_impactassessment.htm

Document Date: March 19, 2012

Document Version: 1.2.0

Name of System: Treasury Collateral Management & Monitoring (TCMM)

SYSTEM GENERAL INFORMATION:

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

TCMM is a centralized application focusing on collateral handling, valuation, and monitoring for the various Treasury business lines: Collections, Cash Management, Bank Management, and other Treasury collateral programs. These business lines are currently embodied in 31 CFR Parts 202 and 225.

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

TCMM system user data is the only information in the system related to individuals. The system user data includes: name, office phone, office email address. This information is used for the operations staff to contact agency and Financial Institution (FI) personnel to resolve collateral issues.

a. Is the information about members of the public?

Yes, but only identifies individuals acting in their professional capacity, with the identifiable information identifying the individuals' office contact information.

b. Is the information about employees or contractors?

Yes.

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

The following regulatory codes give FMS the authority to develop and implement the TCMM system:

31 CFR 202: Depositaries and Financial Agents of the Federal Government

The regulation in this part governs the designation of Depositories and Financial Agents of the Federal Government, and their authorization to accept deposits of public money and to perform other services as may be required of them. Public money includes, but is not limited to, revenue and funds of the United States, and any funds the deposit of which is subject to the control or regulation of the United States or any of its officers, agents, or employees.

31 CFR 225: Acceptance of Bonds Secured By Government Obligations in Lieu of Bonds With Sureties

The regulation in this part governs the acceptance of bonds secured by Government obligations in lieu of bonds with sureties. Persons required by Federal law to give an agency a surety bond instead may provide a bond secured by Government obligations.

31 CFR 380: Collateral Acceptability and Valuation

The regulation in this part governs the acceptability and valuation of all collateral pledged to secure deposits of public monies and other financial interests of the Federal Government under Treasury's Fiscal Service collateral programs.

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Check all that
apply:

Employees

Contractors

Taxpayers

Others (describe)

Agency User -- The Agency user can view and manage information pertaining to their agency. This includes updating the Amount to be Collateralized (ATBC) for their respective FIs. They can also lookup information and access reports about what has been pledged to them.

Local Security Administrator (LSA) Role - The LSA manages users within their own organization. This allows them to create, disable, and reset passwords for their own users.

Report User (Bureau of Public Debt & Office of Fiscal Assistant Secretary) – These users are from BPD and OFAS and can only access certain reports.

Financial Institution (FI) User – The FI User can view information about their account and look at reports pertaining to their institution.

2) **Identify the sources of information in the system**

Check all that apply:

- Employee
- Public
- Federal agencies
- State and local agencies
- Third party

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

From Federal agency employees including FMS, TCMM collects ATBC information and user information, which are voluntarily given by the system users in the course of their professional responsibilities. FRB operations staff inputs ACH payment account information provided by security account holders, all of which are corporations.

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

TCMM does not collect data directly from individuals of the general public.

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

Any Federal agency may utilize TCMM. However, the only information agencies provide are agency user information and ATBC.

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

No State or local agency provides data for use in TCMM.

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

TCMM interfaces with CMS (the FRS collateral system).

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

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

Collateral values pledged by an FI through Federal Reserve collateral systems and displayed in TCMM are accurately valued in CMS, which is the system of record for collateral security transactions. Also, Federal agencies are responsible for managing their deposit information to

accurately report the ATBC within TCMM. The system then performs comparisons in order to monitor deficiencies. In terms of user information, both the Federal agency and FRB operations staff are responsible in verifying that the data collected in the system is accurate and complete.

b. How will data be checked for completeness?

The Federal agency must ensure that the correct ATBC has been reported, which shows the FI the minimum amount of collateral to pledge. TCMM will record a deficiency whenever the FI pledges less than the ATBC according to CMS valuation. In terms of user information, both the Federal agency and FRB operations staff are responsible in verifying that the data collected in the system is accurate and complete.

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

The collateral values provided by CMS are provided on a near real-time basis. Upon the change of values, an automated compare and notification of deficiency occurs.

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

All requirements are defined in use cases and within each use case is a field list describing each field within the user interface.

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 the system as previously detailed in this document is relevant and deemed necessary for the purpose of comparing collateral values against ATBC, reporting deficiencies, and meeting the mission of the Treasury collateral programs.

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?

No.

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

No.

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?

N/A

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

N/A

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.)

The data is retrieved by FI Name or agency security account code. User profile information is only accessible through the organization they are associated with.

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

None.

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?

Individuals (Federal agency employees, FRB support staff, FI users) with access to TCMM utilizes the system only in their professional capacity to perform work-related functions, and are not presented with questions of personal and private matter.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

TCMM has a defined Retention Plan with different types of data being retained for different periods of time. The data within the database is defined to be kept for a total of 7 years with 18 months of those 7 years to be online and available offline for the remaining 5.5 years. As long as the litigation (Cobell) continues, the data will be kept offline indefinitely.

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

The Retention Plan specifics that reports are kept for a minimum of 90 days but it could be longer and that each report specification document states how long the report needs to be kept for.

- 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?

TCMM resides in an infrastructure with one hot site and one back-up site. Replication occurs between the two sites. The IT infrastructure is responsible for replication of the data and moving to the back-up site in a fail-over situation.

- 4) Is the system using technologies in ways that Fiscal Service 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

Users

Managers

System Administrators

System Developers

Others (explain) _____

FMS users, Federal agency users and FI users who have appropriate levels of access and functionality may access the system. Also included is the FRB operations staff, consisting of system administrators and developers, as well as the CBAF.

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

TCMM uses role based security specifying what the user has access to. The user provisioning system requires two individuals to grant this user access.

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

No, the access is restricted. The data accessible to users depends on their roles within the business process, as well as the level of access and functionality permitted to them as defined within the TCMM system.

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)

TCMM users role-based security and applies least privileged access to only give users access to what they need to perform their job.

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?

The Federal Reserve Bank of Philadelphia was involved in the design and development of the system and they are acting as a fiscal agent with appropriate agreements in place. FRB Philadelphia also employs contractors who assist with system development. They signed agreements with confidentiality clauses in compliance with applicable laws.

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

_yes

_X_no

If yes,

a. Explain the interface.

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

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.

Federal agencies have the capability to update/view ATBC, access reports, view account profiles. However, they are restricted in these actions to their own agency with view-shields and functionality defined for the agency.

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

Users have access to their own data and are responsible for the protection of that data. Otherwise, it is up to the ISSO to ensure proper security safeguards, and the FRB operations staff to ensure data quality.

