Treasury Retail Securities Software Application (TRSSA) / Treasury Services Contact Center (TSCC)

Privacy Impact Assessment (PIA)

August 30, 2012

System Information

Name of System, Project or Program: Treasury Services Contact Center (TSCC)
OMB Unique Identifier: 015-35-01-14-02-1020-00

Contact Information

1. **Who is the person completing this document? (Name, title, organization, phone, email, address).**

   Brian Duncan
   Manager
   Treasury Retail Securities
   Federal Reserve Bank of Minneapolis
   Phone: 800-553-2663
   Email: Brian.Duncan@mpls.frb.org
   90 Hennepin Ave.
   Minneapolis, MN 55401

2. **Who is the system owner? (Authorizing Official Name, title, organization, phone, email, address).**

   Paul V. Crowe
   Assistant Commissioner
   Office of Retail Securities
   Bureau of the Public Debt
   Phone: 304-480-6516
   Email: Paul.Crowe@bpd.treas.gov
   200 Third Street, Room 501
   Parkersburg, WV 26106-1328

3. **Who is the system manager? (Name, title, organization, phone, email, address).**

   Brian Duncan
   Manager
   Treasury Retail Securities
   Federal Reserve Bank of Minneapolis
   Phone: 800-553-2663
   Email: Brian.Duncan@mpls.frb.org
   90 Hennepin Ave.
   Minneapolis, MN 55401

4. **Who is the Bureau Privacy Act Officer who reviewed this document? (Name, title, organization, phone, email, address).**

   David Ambrose
   Chief Information Security Officer
   Privacy Officer
   Financial Management Service &
   Bureau of the Public Debt
   Phone: 202-874-6488
   Email: David.Ambrose@fms.treas.gov
   3700 East-West Highway
   Hyattsville, MD 20782

5. **Who is the IT Reviewing Official? (CIO Name, title, organization, phone, email, address).**

   Kimberly A. McCoy
   Chief Information Officer
   Assistant Commissioner
   Office of Information Technology
   Bureau of the Public Debt
   Phone: 304-480-6988
   Email: Kim.McCoy@bpd.treas.gov
   200 Third Street, Room 302
   Parkersburg, WV 26106-1328

System Application/General Information

1. **Does this system contain any information in identifiable form?**

   Yes.

2. **What is the purpose of the system/application?**

   The Treasury Services Call Center (TSCC) system records phone calls and screen shots of computer screens to monitor Treasury Retail Securities customer service representatives. In addition, statistical information related to each call is accumulated for operational purposes.

3. **What legal authority authorizes the purchase or development of this system/application?**

   5 U.S.C. §301; 31 U.SC. §3101, *et seq*

4. **Under which Privacy Act SORN does the system operate? (Provide the system name and unique system identifier.)**

   The system operates under the following SORNS:
   - BPD.001 – Human Resources and Administrative Records
   - BPD.002—United States Savings-Type Securities
   - BPD.003—United States Securities (Other than Savings-Type Securities)
   - BPD.008—Retail Treasury Securities Access Application
   - BPD.009—U.S. Treasury Securities Fraud Information System.

Data in the System

1. **What categories of individuals are covered in the system?**

   Individuals include Retail securities customers or contacts, owners of U.S. Savings Securities, and employees of the Federal Reserve Bank of Minneapolis (FRB Minneapolis).

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

   The sources of information in the system include phone calls and the following systems: TRES Siebel, TreasuryDirect, Legacy Treasury Direct, and HH/H.

   a. **Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

      The system records customer interactions (phone calls and screen shots from various applications listed above) and logs statistical information about each call. No information from individuals is directly entered into the system.

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

      Public Debt and FRB Minneapolis (acting as a fiscal agent under the auspices of Public Debt) are providing data for use in the system.

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

      None.

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

None.

e. What information will be collected from the employee and the public?

The system records customer interactions (phone calls and screen shots) and logs statistical information about each call. No information from individuals is directly entered into the system.

3. Accuracy, Timelines, and Reliability

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

Data is not collected from other sources.

b. How will data be checked for completeness?

Data is not collected from other sources.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models.)

Data is not collected from other sources.

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

Data is not collected from other sources.

Attributes of the Data

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

Yes.

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

No.

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

   Not applicable because no new data will be derived or created.

4. **Can the system make determinations about employees/public that would not be possible without the new data?**

   Yes. The system is used to monitor employee performance.

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

   Not applicable because no new data will be derived or created.

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

   Data is not being consolidated.

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 being consolidated.

8. **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

   Data is retrieved by customer service representative through the monitoring application. The information is used to monitor the performance of the customer service representative and track operational performance.

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

   Reports on employees can be created. The information is used to monitor the performance of the customer service representative and track operational performance. Only FRB Minneapolis management, FRB Minneapolis analysts, and FRB Minneapolis telecom staff have access to the data.

Maintenance and Administrative Controls

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

The system is exclusively used at FRB Minneapolis.

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

   Records of holdings, forms, documents, and other legal papers, which constitute the basis for transactions subsequent to original issue, are maintained for such time as is necessary to protect the legal rights and interests of the United States Government and the person affected, or according to their respective retention schedules.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

   Treasury Retail Securities staff is responsible for obtaining the proper approvals prior to disposition of the data by the IT department. Recorded calls are stored in the contact store and are retained for 14 months. A certain percentage of calls (approximately 30%) are stored with screenshots in the quality monitoring software and are retained for 3 months.

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

   No.

5. **How does the use of this technology affect public/employee privacy?**

   The software enables the FRB Minneapolis to monitor the activities (phone calls and screen shots) of customer service representatives in the Contact Center.

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

   Yes. The software enables the FRB Minneapolis to monitor the activities (phone calls and screen shots) of customer service representatives in the Contact Center.

7. **What kinds of information are collected as a function of the monitoring of individuals?**

   The software records phone calls and screen shots of individuals working in the Contact Center.

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

   Only authorized FRB Minneapolis management, FRB Minneapolis analysts, and FRB Minneapolis telecom staff have access to the data. Standard controls such as password mechanisms are in place to prevent unauthorized monitoring.

9. **If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.**

   The system is not currently being modified.

Access to Data

1. **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others.)**

   Data is available to TRS management, TRS analysts, and FRB Minneapolis telecom staff.

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

   Access is driven by the role of the user and their position as it relates to the Retail Securities business. Procedures are in place to manage the access process whereby the Treasury Retail Securities management staff authorize/request access for individuals.

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

   The system employs a role-based access model. Staff are placed in groups according to the business need.

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

   a. All FRB Minneapolis employees are required to adhere to their Information Security Policy.
   b. Data security and valuables handling training sessions are conducted annually for all TRS Department employees.
   c. All TRS employees complete an on-line training course to comply with the "Sensitive But Unclassified" mandate.
   d. All TRS employees complete the annual *Information Security: Security Matters* and *Treasury Privacy Matters* on-line training courses.
   e. Users follow Rules of Behavior.
   f. FRB Minneapolis personnel are subject to background investigations and periodic re-investigations as a condition of employment.
   g. Other mitigating controls include Security Assessment and Authorizations, and Continuous Monitoring.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

   No. This is an existing off-the-shelf product.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

   No.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   All employees with access to the system or data produced by the system are responsible for protecting the privacy rights of the public. Employees affected by the interface are protected in accordance with information classification and handling policies.

8. **Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?**

   FRB Minneapolis.

9. **How will the data be used by the other agency?**

   Data is used exclusively by FRB Minneapolis to monitor performance of employees working in the Contact Center.

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

    All employees with access to the system or data produced by the system are responsible for assuring proper use of the data in accordance with information classification and handling policies.