Treasury Retail E-Services (TRES)
Privacy Impact Assessment (PIA)

September 29, 2011

System Information

Name of System, Project, or Program: Treasury Retail E-Services (TRES)
OMB Unique Identifier: 015-35-01-14-02-1006-00

Contact Information

1. **Who is the person completing this document? (Name, title, organization, phone, email, address).**
   Dana Keeley
   Business Analyst
   Treasury Retail Securities
   Federal Reserve Bank of Minneapolis
   651-726-3104
   Dana.Keeley@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
   304-480-6516
   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
   651-726-3091
   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
   202-874-6488
   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
   304-480-6988
   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?**
   Treasury Retail E-Services (TRES) is a multi-channel customer service solution that manages and tracks all retail customer interactions across both Treasury Retail Securities (TRS) sites at the Bureau of the Public Debt (Public Debt) and the Federal Reserve Bank of Minneapolis (FRB Minneapolis).

   TRES supports the delivery of high quality, consistent, and efficient customer service for all Retail Securities' inquiries from account holders and the general public. TRS customer service representatives at both sites have a fully integrated view of the customer and their past interactions. Information processed and/or stored by TRES includes customer or contact names, mailing addresses, e-mail addresses, phone numbers, Social Security Numbers (SSN), account numbers from some legacy systems, and other customer case file information.

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.)**

   TRES operates under the following SORNs:
   - 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?**
   Retail securities' customers or contacts – owners or inquiries of U.S. savings securities, U.S. Treasury marketable securities and other non-marketable federal debt obligations managed by Retail are the categories of individuals.

2. **What are the sources of the information in the system?**
   The sources of information in the system include customer or contact mail, e-mail, phone calls, and the following Public Debt applications: Bureau Automated Tracking System, TreasuryDirect, Legacy Treasury Direct, HH/H System, REGII System. Data converted from the FRB Minneapolis Interaction Center – Call Center Queue (IC/CCQ) is also a source of the information in the system.

   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?**
      Information is received and entered into the system from paper requests, e-mail requests, or phone calls where the caller verbally shares the information with a customer service representative. Other sources of information include the following Public Debt applications: Bureau Automated Tracking System, TreasuryDirect, Legacy Treasury Direct, HH/H System, and REGII System. Data converted from FRB Minneapolis IC/CCQ is also a source of information.

   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?
Information collected from the employee and the public include customer or contact name, mailing address, e-mail address, phone numbers, SSN, account numbers from some legacy systems, and other relevant information to assist the customer.

3. Accuracy, Timelines, and Reliability

a. How will data collected from sources other than bureau records be verified for accuracy?
Customer service representatives will verify the accuracy of key data each time the customer or contact calls, e-mails, or sends correspondence to FRB Minneapolis or to the Office of Retail Securities.

b. How will data be checked for completeness?
Each TRES Service Request in the application is updated to denote actions completed and is closed out when completed.

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 current within each request. Customer service representatives will verify the accuracy of key data each time the customer makes an inquiry.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?
Yes. The data elements are described in detail and documented in the Siebel Data Dictionary.

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?
No.

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. Access is controlled by Public Key Infrastructure (PKI) certificates at the FRB and through Personal Identity Verification (PIV) cards at Public Debt.

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 can be retrieved by customer or contact name, SSN, phone number or e-mail address.

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 are available to show the number of inquiries made by an individual and the details of each inquiry. These reports are for internal use only. All staff with the appropriate access to TRES have the ability to retrieve the reports.

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 operated at one site – Treasury Web Application Infrastructure (TWAI).

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?**
   At this time, there are no plans to delete or archive data from the Siebel database. All reports are run on demand from the data warehouse and all data is being retained. Procedures are not necessary at this time.

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?**
   This does not apply based on the response to question number four.

6. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
   When a customer or contact contacts TRS or Public Debt by e-mail or phone, the system attempts to identify the customer or contact using the telephone number or e-mail address. The customer or contact address on file is used to mail information to the customer or contact. The system cannot be used to monitor individuals.

7. **What kinds of information are collected as a function of the monitoring of individuals?**
   None.

8. **What controls will be used to prevent unauthorized monitoring?**
   Employees and agents of Public Debt are subject to personnel screening procedures. Information stored in electronic media is safeguarded by automatic data processing security procedures in addition to physical security measures. For those categories of records stored in computers with online terminal access, the information cannot be accessed without proper passwords and preauthorized functional capability.

9. **If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.**
   Yes. Any needed SORN updates will be addressed appropriately.

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 the Public Debt Retail Securities staff, TWAI support staff, FRB developers, and FRB contractors.

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 Public Debt Retail Securities management staff at each site authorize/request access for staff. Public Debt staff uses PIV cards, and FRB staff use PKI credentials to authenticate to the system.

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 is placed in groups according to the business need. Some roles allow access to customer data while others may be administrative roles.

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.)**
   - All FRB Minneapolis employees are required to adhere to their Information Security Policy.
   - Data security and valuables handling training sessions are conducted annually for all TRS Department and Public Debt employees.
   - All TRS and Public Debt employees completed an on-line training course to comply with the "Sensitive But Unclassified" mandate for Federal Reserve Banks.
   - All TRS employees completed the annual *Information Security: Security Matters* and *Treasury Privacy Matters* on-line training courses.
   - All Public Debt employees are required to take periodic training in *Computer Security Awareness*.
   - Users follow Rules of Behavior (e.g. FRB Minneapolis and Public Debt Code of Conduct).
   - Public Debt and FRB Minneapolis personnel are subject to background investigations and periodic re-investigations as a condition of employment.

   Other mitigating controls include Security Assessment and Authorization, 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?**
   Contractors are restricted to the development of the system. FRB Minneapolis, however, will perform system maintenance. The contract contains a confidentiality clause and also requires each contractor to sign a non-disclosure agreement for both FRB Minneapolis and Public Debt**.** The non-disclosure agreement references the Privacy Act and other statutory and regulatory measures.

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)?**
   No.

9. **How will the data be used by the other agency?**
   Other agencies will not have access to TRES data.

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.