Legacy Treasury Direct®
Privacy Impact Assessment (PIA)

September 1, 2007

System Information

Name of System, Project or Program: Legacy Treasury Direct
OMB Unique Identifier: 015-35-01-01-02-1011-00

Contact Information

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

   Patrick H. Ahlborn
   Division Director/Project Manager
   Office of Retail Securities/Division of Records Systems
   (304) 480-6272
   Pat.Ahlborn@bpd.treas.gov
   200 Third Street, Room 502
   Parkersburg, WV 26106-1328

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

   John R. Swales III
   Assistant Commissioner
   Office of Retail Securities
   304-480-6516
   John.Swales@bpd.treas.gov
   200 Third Street, Room 501
   Parkersburg, WV 26106-1328

3. **Who is the system manager? (Name, title, organization, phone, email, address).**
   Adrienne Murphy, Project Manager LTD
   CBAF – Central Business Application Function
   FRB of Philadelphia
   Office: 215.574.3911
   Adrienne.murphy@phil.frb.org

4. **Who is the Information Systems Security Manager who reviewed this document? (ISSM Name, title, organization, phone, email, address).**
   Jim McLaughlin
   Information Systems Security Manager
   Division of Program Services
   (304) 480-7972

Jim.mclaughlin@bpd.treas.gov
200 3rd Street Room 409
Parkersburg, WV 26106-1328

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

Denise K. Hofmann
Disclosure Officer
Office of Management Services
(304) 480-8402
Denise.Hofmann@bpd.treas.gov
200 Third Street, Room A4-A
Parkersburg, WV 26106-1328

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

Kimberly A. McCoy
Assistant Commissioner
Office of Information Technology
(304) 480-6635
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. Personal investor data is stored within the application and is viewable via on-line inquiries and paper documents (i.e., statements of account, confirmation of transaction notices, tax statements) containing said data is generated and mailed to investors**.** Personal data such as investor account number or SSN may also appear on system reports used to record and verify the completed transaction.

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

The Legacy Treasury Direct application is an automated system for the issuance, maintenance, payment and redemption of Treasury securities for investors who wish to deal directly with the U.S. Treasury. The Legacy Treasury Direct application also provides payment and tax reporting services to other offices within the Treasury Department and to the Treasury Retail Securities Sites.

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

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

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

   Treasury/BPD.003 United States Securities (Other than Savings-Type Securities)

Data in the System

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

   Individual investors as well as corporations are covered in the system.

2. **What are the sources 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?**

      The source of information is taken directly from the investor.

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

      Payment and tax reporting data is provided by other offices within the Treasury Department. FRB'S Pittsburgh and Minneapolis plus BPD?

   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 Legacy Treasury Direct application gathers and stores the following data from investors: Name, address, telephone numbers (primary and secondary), SSN, account number, security term, purchase amount, transfer information, personal bank information such as bank name, ABA routing number, bank account number and type of account such as

checking or savings. System users have their SSN and access data (such as user ID) recorded.

3. **Accuracy, Timelines, and Reliability**
   a. **How will data collected from sources other than bureau records be verified for accuracy?**

      Data pertaining to an investor's transaction may be verified manually by comparing system output records against actual source documents. For more sensitive transactions the system requires two separate operators for the processing and verification of the transaction.

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

      All processed transactions are recorded on system reports that may be used to check for completeness. In addition, most completed transactions are recorded on system advices.

   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.)**

      Most completed transactions are recorded historically on an investor statement of account which is issued each time the transaction is processed successfully. The statement of account contains investor data such as name, address, SSN (ONLY FIRST TIME AND THEN AFTER SHOWS CONFIDENTIAL) and personal banking information. Other notices containing similar personal data confirming transactions are also mailed to the investor. The investor reviews this information and would be responsible for notifying us of any updates.

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

      All data elements pertaining to system output such as statements of account and confirmation notices are recorded in program libraries within the application.

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?**
   Data is collected to allow for the issuance, maintenance, payment, and redemption of Treasury Securities for investors.

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?**

   The only information entered and maintained in the system is the data entered by the system user necessary to process a requested transaction. Any updates to investor personal data would be sanctioned only by the investor. No additional updates are made automatically to an account. Any authorized updates to personal data are recorded historically by separate history records which outline each update and are dated and bear the user ID of the person processing the updates. The system does not process aggregated data.

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

   All updates to investor data are recorded in the appropriate databases**.**

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

   No. The system only processes authorized data.

5. **How will the new data be verified for relevance and accuracy?**
   All data entered is authenticated for relevancy and accuracy by authorized individuals.

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

   Public Debt implements NIST SP 800-53 and TD P 85-01 security controls to protect data from unauthorized access or use. Other mainframe security controls are in place such as user role based access controls.

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

   Yes. Public Debt follows NIST SP 800-37 for certification and accreditation. Certification and Accreditation is performed every 3 years. In between those years Public Debt performs continuous monitoring to ensure the proper controls are in place and functioning as expected.

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.**
   Personal data is retrieved by entering an investor's account number or SSN. Inquiry into an investor's account may only be performed by an authorized user. Paper documents are generated and mailed to the investor. Data appearing on

paper documents such as statements or confirmation notices may be viewed on-line for only 30 days.

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

   System reports reflect a listing of transactions that were processed successfully. These reports are used for verification of the transaction or financial settlement. System output pertaining to individual investors is limited to statement of accounts, tax statements and confirmation notices of investor transactions. Only authorized system users with the appropriate access may view this 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?**

2. The Legacy Treasury Direct application resides in a centralized environment located at the Federal Reserve Data Center in East Rutherford, NJ. Consistent use of the system and data is controlled through mainframe security and user role based access.
   Payment and data related to investor holdings are maintained within the application for 18 months following a redemption cycle.

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?**

   Data purged from the application is written to magnetic tapes that are forwarded to the Bureau of the Public Debt for loading into their mainframe system. Data disposition is determined by the Bureau of the Public Debt and would follow their procedures for its disposal.

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?**

   Legacy Treasury Direct adheres to Privacy Act restrictions. Access to sensitive investor data is granted only to authorized system users with the appropriate access. The Legacy Treasury Direct application also complies with Federal Reserve System standards for the classification and handling of sensitive data.

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

Yes. The security controls for Legacy Treasury Direct provide the capability to monitor individual users and unauthorized attempts.

7. **What kinds of information are collected as a function of the monitoring of individuals?**
   Reports used in the monitoring of security access reflect the name and user ID and a description of the attempted transaction.

8. **What controls will be used to prevent unauthorized monitoring?**
   Legacy Treasury Direct information is contained in secure buildings or in areas which are occupied either by officers and responsible employees of Public Debt and the Federal Reserve Bank who are subject to personnel screening procedures. Additionally, since in most cases, numerous steps are involved in the retrieval process, unauthorized person would be unable to retrieve information in meaningful form. Information stored in electronic media is safeguarded by automatic data processing security procedures in addition to physical security measures.

   Authorized Federal Reserve Bank (FRB) users of the Legacy Treasury Direct application must adhere to FRB's Code of Conduct as well as attend an Ethics training course.

9. **Under which Privacy Act SORN does the system operate? Provide number and name.**

   Treasury/BPD.003 United States Securities (Other than Savings-Type Securities)

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

    The system is not currently undergoing a revision. Any updates to the Privacy Act SORN will be addressed as needed.

Access to Data

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

   Internal users, system administrators and developers

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

User access is determined by security controls monitoring the Legacy Treasury Direct system. Users are granted access based on their job duties.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**
   Data access is restricted to an "as needed only" basis in compliance with their job responsibilities.

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.)**

   Daily monitoring of access is provided by the Legacy Treasury Direct CBAF and reviewed by its management. Every authorized user of the Legacy Treasury Direct application is given an access role controlled by the responsibilities of their particular job. No one user has unlimited access. In addition, the Legacy application has an operator capability matrix which is controlled and maintained by the security administrator of the user site. All users are subject to a Code of Conduct and Ethics training course.

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. Contractors are not involved**.**

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

   Yes, Electronic Services for Treasury Bills, Notes, and Bonds (ESTBNB) and TDFeeS interface with Legacy Treasury Direct.

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

   Although Legacy Treasury Direct does not have any interface with any other systems. All employees who access the Legacy Treasury Direct system have the responsibility to protect the privacy rights of the public.

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

   Currently, active authorized user sites for the Legacy Treasury Direct application include the Federal Reserve Banks of Pittsburgh and Minneapolis in addition to

the Bureau of the Public Debt. The Federal Reserve Bank of Philadelphia is responsible for the administrative as well as CBAF activities.

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

The Federal Reserve Banks and Public Debt access the data within the Legacy application to service investors.

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

Employees who have access to the system, the system manager, system owner and ultimately the Bureau CIO are responsible for assuring the proper use of data in the system.

The Public Debt Disclosure Officer is responsible for administering requests for system data submitted to the Bureau involving the Privacy Act. Public Debt fully complies with the provisions of the Freedom of Information Act (FOIA), Title 5 U.S.C. Section 552, and the Privacy Act, Title 5 U.S.C. Section 552a. Public Debt provides an established procedure to solicit requests to review and correct information recorded, and we have a dedicated Disclosure Officer who manages and administers the program.