Legacy Treasury Direct®
Privacy Impact Assessment (PIA)

January 15, 2010

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).**

   Glenn Siber
   Manager, Mainframe Systems Branch
   Office of Retail Securities/Division of Records Systems
   (304) 480-7599
   Glenn. Siber@bpd.treas.gov
   200 Third Street
   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
   Parkersburg, WV 26106-1328

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

   Adrienne Murphy, Project Manager, Legacy Treasury Direct (LTD)
   CBAF – Central Business Application Function
   FRB of Philadelphia
   Office: 215-574-3911
   Adrienne.murphy@phil.frb.org
   10 Independence Mall
   Philadelphia, PA 19105

4. Who is the Information Systems Security Manager who reviewed this document? (ISSM Name, title, organization, phone, email, address).

Jim D. McLaughlin
Chief Information Security Officer / Privacy Act Officer
Division of Program Services
(304) 480-7972
Jim.mclaughlin@bpd.treas.gov
200 3rd Street
Parkersburg, WV 26106-1328

5. 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
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?

- Bureau of the Public Debt
- Federal Reserve Bank of Philadelphia
- Federal Reserve Bank of Minneapolis
- Federal Reserve Bank of Cleveland - Pittsburgh Branch
- Federal Reserve Bank of Chicago

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 or EIN, 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, and tax information. 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 and bank account number. 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. Data elements pertaining to each notice or statement are documented in a form profile within these program libraries.

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. The 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?

Yes. Electronic Services for Treasury Bills, Notes, and Bonds (ESTBNB) and the data entry reinvestments and ESTBNB fee payment requests are collected each business day and transmitted via Connect:Direct; mainframe file transfer utility. These files are uploaded into Legacy Treasury Direct®. These daily files are saved in Legacy Treasury Direct for a month. Any updates to investor personal data would be sanctioned only by the investor. The Notification of Change (NOC), where a financial institution requests changes to an investor's direct deposit information, comes directly into Legacy Treasury Direct and an authorized user can accept, cancel, or reject the transaction. Upon approval of the NOC, the account will be updated to show the change. NOC files are saved for a month in Legacy Treasury Direct. Any authorized updates to personal data are

recorded historically by separate history , which highlight each update and are dated and bear the user identification of the person processing the updates.

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

   All updates to investor data are recorded and confirmed to the investor and are stored 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 employees of the Bureau of the Public Debt (BPD) and the Federal Reserve Banks.

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

   BPD 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. BPD follows NIST SP 800-37 for certification and accreditation. Certification and Accreditation is performed every 3 years. In between those years BPD 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 into the system. 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?**

   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. Legacy Treasury Direct's contingency site is in Dallas where every night the latest set of images are loaded onto their mainframe. The database is restored twice a year for the Business Resumption Testing to ensure everything is working properly.

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

   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 transferred via Connect:Direct to BPD for loading into their mainframe system. Data disposition is determined by BPD and would follow its 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 identification 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 BPD 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.)**

   Users, system administrators and developers.

   These records may be disclosed to:
   - Agents or contractors of the Department for the purpose of administering the public debt of the United States;
   - Next-of-kin, voluntary guardian, legal representative or successor in interest of a deceased or incapacitated owner of securities and others entitled to the reissue, distribution, or payment for the purpose of assuring equitable and lawful disposition of securities and interest;
   - Either co-owner for securities registered in that form or to the beneficiary for securities registered in that form, provided that acceptable proof of death of the owner is submitted;
   - The Internal Revenue Service (IRS) for the purpose of facilitating collection of the tax revenues of the United States;
   - The Department of Justice in connection with lawsuits to which the Department of the Treasury is a party to trustees in bankruptcy for the purpose of carrying out their duties;
   - The Veterans Administration and selected veterans' publications for the purpose of locating owners or other persons entitled to undeliverable bonds held in safekeeping by the Department;
   - Other Federal agencies to effect salary or administrative offset for the purpose of collecting debts;
   - A consumer reporting agency, including mailing addresses obtained from the IRS to obtain credit reports;
   - A debt collection agency, including mailing addresses obtained from the IRS, for debt collection services;
   - Contractors conducting Treasury-sponsored surveys, polls, or statistical analyses relating to the marketing or administration of the public debt of the United States;
   - Appropriate Federal, State, local, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statue, rule, regulation, order, or license;
   - A court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena;
   - A Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;
   - Disclose through computer matching, information on individuals with whom the Bureau of the Public Debt has lost contact, to other Federal

agencies for the purpose of utilizing letter-forwarding services to advise these individuals that they should contact the Bureau about returned payments and/or undeliverable securities;
- Debtor information is also furnished, in accordance with 5 U.S.C. 552a(b)(12) and section 3 of the Debt Collection Act of 1982, to consumer reporting agencies to encourage repayment of an overdue debt;
- To appropriate agencies, entities, and persons when the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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 employees on 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 Central Business Administration Function area 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) is a front-end interface to Legacy Treasury Direct®. Electronic Services for Treasury Bills Notes and Bonds utilizes screen-scraping technology to share information with Legacy Treasury Direct. Information is shared back and forth between Electronic Services for Treasury Bills Notes and Bonds and Legacy Treasury Direct.

   Fee payment information is shared back and forth between the Treasury Direct Fee System and Electronic Services for Treasury Bills Notes and Bonds.

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

   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, Minneapolis, and Chicago in addition to BPD. The Federal Reserve Bank of Philadelphia is responsible for the administrative as well as the Central Business Administration Function activities.

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

   The Federal Reserve Banks and BPD 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 Chief Information Officer are responsible for assuring the proper use of data in the system.

BPD's Disclosure Officer is responsible for administering requests for system data submitted to the Bureau involving the Privacy Act. BPD 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. BPD 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.