Electronic Services for Treasury Bills, Notes, and Bonds (ESTBNB)
Privacy Impact Assessment (PIA)

January 15, 2010

System Information

Name of System, Project or Program: Electronic Services for Treasury Bills, Notes, and Bonds (ESTBNB)
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).**

   Greg Sheppard
   Manager, System Analysis and Support Branch
   Division of Records Systems
   304-480-6916
   Greg.Sheppard@bpd.treas.gov
   200 Third Street
   Parkersburg, WV 26106-1328

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

   Michael McDougle
   Director, Division of Records Systems
   304-480-7323
   Michael.McDougle@bpd.treas.gov
   200 Third Street
   Parkersburg, WV 26106-1328

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

   Greg Sheppard
   Manager, System Analysis and Support Branch
   Division of Records Systems
   304-480-6916
   Greg.Sheppard@bpd.treas.gov
   200 Third Street
   Parkersburg, WV 26106-1328

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
Security Program Staff
304-480-7972
Jim.McLaughin@bpd.treas.gov
200 Third 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
304-480-6988
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

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

   ESTBNB is an interactive phone and web service that provides established Legacy Treasury Direct investors the option of purchasing or reinvesting Treasury securities. They can also request a statement of their account, a duplicate interest income statement, their account balance, change their address or phone number, or have their Legacy Treasury Direct account maintenance fee debited from their checking or savings account via an ACH transaction.

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

   5 U.S.C.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?**

   Legacy Treasury Direct account holders.

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?**

      Individual

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

      Bureau of the Public Debt
      Federal Reserve Bank of Philadelphia

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

      N/A

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

      N/A

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

      - Account Number
      - Taxpayer Identification Number (TIN)
      - Address
      - Phone Number
      - Remittance Number
      - Committee on Uniform Security Identification Procedures (CUSIP) Number
      - Security Term
      - Purchase Amount
      - Issue Date
      - Validation Number

3. Accuracy, Timelines, and Reliability

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

Data accuracy is established via internal edit controls, as well as verified with the Legacy Treasury Direct system.

b. How will data be checked for completeness

Data completeness is verified using internal edit controls, as well as verified with valid values in the database or verified with the Legacy Treasury Direct system.

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.)

Yes. System edits and verifications with Legacy Treasury Direct are applied to ensure data is current and not out-of-date.

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

Yes. Electronic Services for Treasury Bills, Notes, and Bonds (ESTBNB) Production Operating Procedures (POP) manual lists required data elements, descriptions, field type and sizes.

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 gives established Legacy Treasury Direct investors the option of purchasing or reinvesting Treasury securities over the telephone or on the internet. They can also request a statement of their account, a duplicate interest income statement, their account balance, change their address or phone number, or have their Legacy Treasury Direct account maintenance fee debited from their checking or savings account via an ACH transaction.
   .

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, purchase information and account service requests are directly entered into the Legacy Treasury Direct system by ESTBNB and logged into a local database table. Reinvestment and fee payment requests are stored in a local database table and transmitted to Legacy Treasury Direct each business day via Connect:Direct file.

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

   The new data will be reflected in the Legacy Treasury Direct system.

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

   Yes, new data will update an individual's record of purchases, reinvestments, fee payments and account service transactions in Legacy Treasury Direct.

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

   Data accuracy is established via internal edit controls, as well as verified with the Legacy Treasury Direct system.

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

   Electronic Services for Treasury Bills, Notes, and Bonds (ESTBNB) data is contained in secure, access-controlled buildings and processing environments. Employees or agents of Public Debt are subject to the Treasury Department Code of Conduct and must undergo periodic personnel screening procedures.

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

   Yes, security controls are reviewed annually. Every three years ESTBNB undergoes a full certification and accreditation following NIST SP 800-37 guidelines.

   During the three-year cycle security controls are reviewed and tested annually. If the system undergoes a change that would impact security then a full new certification and accreditation would be completed.

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 using a personal identifier, which includes Legacy Treasury Direct account number and taxpayer identification number.

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

   No reports on individuals are available directly from the ESTBNB system.

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 maintained at the Bureau of the Public Debt's (BPD) facility and at our off-site backup facility. BPD uses remote copy technology for data replication to our contingency facility. Both sites are operational at all times.

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

   The individual records are maintained in the Legacy Treasury Direct system. Only transactional logs, using key data, are maintained at BPD. The retention period of the transactional logs is 13 months. After 13 months, the data is backed-up to tape and sent to off-site storage for two years.

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?**

   After the tapes are stored off-site for two years, they are brought back to BPD and are overwritten and used again. These procedures are documented in BPD's Office of Information Technology.

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?**

   N/A

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

   No.

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

   N/A

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

   N/A

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 existing Privacy Act system of records, which covers this system, was not substantially revised.

Access to Data

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

   The primary users of data in the system will be:
   - Legacy Treasury Direct account holders

   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?**

   The Legacy Treasury Direct Account Holder has access to their information with the use of identifying information (account number and taxpayer identification number).

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

   The Legacy Treasury Direct account holder only has access to a portion of their individual data. This is restricted through identifying information (account number and taxpayer identification number). Also, Legacy Treasury Direct account holders have the option to block their account from being accessed using ESTBNB.

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.)**

   Security Plan
   Risk Management Plan
   Certification and Accreditation Process
   Security Matrix
   Rules of Behavior

Mandatory Periodic training in Computer Security Awareness
Quarterly Newsletter "Frontline"
Audit Trails/Logs
Continuous Monitoring Process

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, were a Privacy Act contract clause inserted in their contracts and other statutory and regulatory measures addressed?**

   No contractors are involved with the maintenance of the system

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

   Yes.

   ESTBNB is a front-end interface to the Legacy Treasury Direct system. ESTBNB utilizes screen-scraping technology to share information with the Legacy Treasury Direct system. Information is shared back and forth between ESTBNB and Legacy Treasury Direct.

   Fee payment information is shared back and forth between Treasury Direct Fee System (TDFeeS) and ESTBNB.

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

   All BPD employees who have access to information in a Privacy Act system are responsible for protecting personal information covered by the Privacy Act. The information owner, system manager and ultimately the BPD CIO have the responsibility to see that the data is protected from all threats.

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?**

   N/A

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

All BPD employees who have access to the system, the system manager, system owner, and ultimately the BPD CIO are responsible for assuring the proper use of the 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.