BATS—Bureau Automated Tracking System
Privacy Impact Assessment (PIA)

September 1, 2007

System Information

Name of System, Project or Program: BATS—Bureau Automated Tracking System
OMB Unique Identifier: 015-35-01-14-02-1013-00

Contact Information

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

   Patrick H. Ahlborn, Director
   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? (ISSO Name, title, organization, phone, email, address).**

   Patrick H. Ahlborn, Director
   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

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

Jim McLaughlin
Information Systems Security Manager
Office of Information Technology
Division of Program Services
304-480-7972
Jim.McLaughlin@bpd.treas.gov
200 Third 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

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

BATS is a Bureau of the Public Debt (BPD) wide application designed to provide consolidated customer request tracking. BATS processes requests including customer service transactions that contain the customer name, address and taxpayer identification number. Investment information including savings bond serial numbers and marketable security account numbers may be retained. Legal information, such as marriage and death certificates, and citation information, such as GSRS' interpretation of Federal regulations, may also be retained. The

functionality contained in the BATS application can be generally described as: 1) the creation and maintenance of customer information, 2) the creation and maintenance of request information, and 3) the assignment and tracking of work relation to customers and/or requests. BATS does not establish automated interfaces with any other application.

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

   5 U.SC.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.)**

   Treaury/BPD.002 – United States Savings- Type Securities – Treasury/BPD

Data in the System

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

   Present and former owners of, claimants to, persons entitled to, legal representatives of and inquirers concerning United States savings-type securities and marketable securities.

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 or Legal Representative

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

      None

   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?**

Issuance: Records relating to registration, issuance and correspondence in connection with issuance of savings-type securities.

- Name of Registered Owner or First Named Co-owner
- Taxpayer Identification Number (TIN) of the registered owner or first named co-owner
- Name of Beneficiary or Second Named Co-owner
- Taxpayer Identification Number (TIN) of the beneficiary or second named co-owner
- Inscription Address

Holdings: Records documenting ownership, status, payments by date and account number, inscription information, interest activity, non-receipt or over-or-underpayments of interest and principal and numerical registers of ownership.

Transactions (redemptions, payments and reissues): Records, which includes securities transaction requests; interest activity; legal papers supporting transactions; applications for disposition or payment of securities and/or interest thereon of deceased or incapacitated owners; records of retired securities; and payment records.

Claims: Records including correspondence concerning lost, stolen, destroyed, or mutilated savings-type or marketable securities; bonds of indemnity; legal documents supporting claims for relief; and records of caveats entered.

Inquiries: Records of correspondence with individuals who have requested information concerning savings-type securities or marketable securities and/or interest thereon.

3. Accuracy, Timelines, and Reliability

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

The certifying officer must require the person presenting a bond, or appropriate BPD transaction form, to establish his or her identity in accordance with Department of Treasury instructions and identification guidelines.

b. How will data be checked for completeness

The BATS system edits each field to see that the data has the correct type and number of characters and is in the correct format.

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 are applied to ensure data is current and not out-of-date. Out-of-date data is flagged and addressed immediately.

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

Yes. Savings Bond Handbook, Legacy Treasury Direct Handbook, and Retail Handbook with cross-references to the Federal Register, Department Circular (Treasury) and Code of Federal Regulations. The Database Specifications manual lists data elements, field types 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, information in this system of records is collected and maintained to enable Public Debt and its agents to service savings bonds and marketable securities, to process transactions, to make payment, and to identify owners and their accounts.

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, data collected will be used to document ownership, status, payment date, inscription information, interest activity, non-receipt or over or under payments of interest and principle and numerical register of ownership. Data is stored on paper, microfilm or electronic media.

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

   The data is placed in an existing file system with information on the individual (e.g. tax identification numbers, inscription address, etc.)

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 records of issuance, holdings, transactions or claims.

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

System edits are applied to ensure data is current and not out-of-date. Out-of-date data is flagged and addressed immediately

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

BATS data is contained in secure buildings and processing environment. Employees or agents of Public Debt are subject to the Treasury Department Code of Conduct and must undergo periodic personnel screening procedures.

Numerous steps are involved in the data retrieval process; unauthorized persons 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.

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

Yes. The programming code for BATS can only be modified by the Office of Information Technology, Division of Systems Development (DSD). All changes made to the system's programming code (fixes, updates and inclusion of new functionality) are managed in accordance with existing DSD procedures and practices.

These controls are used to monitor the installation of, and updates to, application software to ensure that the software functions as expected when other software is installed on the system.

All programming changes undergo a regimented testing protocol before they are deployed into Production. OIT programmers perform initial testing of the code in the Integration region. If the code passes Integration testing, then it is migrated to the Acceptance region where Retail staff performs more rigorous testing. Only after the code successfully passes Acceptance region testing, is it migrated to production. Management controls and operating procedures exist throughout the migration process to ensure that the protocol is strictly followed. Following acceptance testing, OIT's Tech Lab performs load testing on the program under a simulated production environment. This testing is performed to determine if the revised programming code can withstand public use without decreased performance.

All data changes not made through system interfaces are coordinated by DSD and fully documented using the BPD AD-HOC Change Request Form or the BPD Data Move Request Form. Also prior to each release, both Retail and SAB personnel test all IT security controls within the system.

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 in a number of ways using a personal identifier. Information can be retrieved by bond serial number or by taxpayer identification number (social security number or employer identification number). To a limited extent, information can be retrieved by name and address of the registered owner or first named coowner.

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

   Information regarding requests received and processed is necessary to maintain good customer service and meet the standards set for timely processing of work. The reports available from BATS provide the means to:

   - Monitor and evaluate Bureau performance
   - Review employee assignments and performance
   - Track the location of physical customer casefiles and request

   The "roles" assigned to the user determine access to 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 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 backup facility.

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 otherwise until they are no longer historically significant.

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?**

   Other records are disposed of at varying intervals in accordance with records retention schedules reviewed, approved, and documented by the National

Archives and Records Administration (NARA). Paper and microfilm records are destroyed via shredding or maceration. Records in electronic media are electronically erased using accepted techniques.

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

   User access is restricted. Safeguards are in place to only allow users of the system to have access to the data they need to perform their job duties.

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

   Not applicable

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

   Yes, information in this system of records is collected and maintained to enable Public Debt and its agents to service savings bonds and marketable securities, to process transactions, to make payments, and to identify owners and their accounts.

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

   Information in this system of records is collected and maintained to enable Public Debt and its agents to service savings bonds and marketable securities, to process transactions, to make payments, and to identify owners and their accounts.

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

   Information is contained in secure buildings or in areas which are occupied either by officers and responsible employees of Public Debt who are subject to personnel screening procedures and to the Treasury Department Code of Conduct or by agents of Public Debt who are required to maintain proper control over records while in their custody. Additionally, since in most cases, numerous steps are involved in the retrieval process, an 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. 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. **Under which Privacy Act SORN does the system operate? Provide number and name.**

Treaury/BPD.002 – United States Savings- Type Securities – Treasury/BPD

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 in FY06 or FY07.

Access to Data

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

The users of the system are BPD employees including: operators, managers, system administrators, and developers.

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

Information is contained in secure buildings or in areas which are occupied either by officers and responsible employees of Public Debt who are subject to personnel screening procedures and to the Treasury Department Code of Conduct or by agents of Public Debt who are required to maintain proper control over records while in their custody. Additionally, since in most cases, numerous steps are involved in the retrieval process, an 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. For those categories of records stored in computers with online terminal access, the information cannot be accessed without proper passwords and preauthorized functional capability. BPD maintains documented procedures concerning controls and responsibilities regarding access.

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

User access is restricted. Safeguards are in place to only allow users of the system to have access to the data they need to perform their job duties.

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
Certification and Accreditation Process
BATS Organizations and Roles
Rules of Behavior
Mandatory Periodic Training in Computer Security Awareness

Quarterly Newsletter "Frontline"
ISSR Monthly Newsletter
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, was Privacy Act contract clauses 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.**

   No

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)?**

   None

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

   Not Applicable

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 data in the system.

    The Public Debt Disclosure Officer is responsible for administering requests for system data submitted to BPD 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.