EZ Clear Privacy Impact Assessment (PIA)

September 1, 2007

System Information

Name of System, Project or Program: EZ Clear
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).**

   Chris Poirier
   Senior Business Analyst, Treasury Retail Securities Department
   Federal Reserve Bank of Cleveland, Pittsburgh Office
   412-261-7808
   cpoirier@clev.frb.org
   717 Grant Street
   Pittsburgh, PA 15219

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).**

   Jill A Krauza
   Assistant Vice President
   Federal Reserve Bank of Cleveland, Pittsburgh Office
   412-261-7991
   jkrauza@clev.frb.org
   717 Grant Street
   Pittsburgh, PA 15219

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
   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
2. **What is the purpose of the system/application?**
   Process redeemed savings bonds and produce supporting files and documentation for the Bureau of the Public Debt.

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.)**

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

Data in the System

1. **What categories of individuals are covered in the system?**
   Any individual that has redeemed a U.S. Savings Bond.

2. **What are the sources of the information in the system?**
   Financial institutions deposit redeemed savings bonds through their local Federal Reserve Office or directly to the Federal Reserve Bank of Cleveland, Pittsburgh Branch.

   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 information is taken from the individual's redeemed savings bond.

   b. **What Federal agencies are providing data for use in the system?**
      Bureau of the Public Debt

   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 savings bond serial number and redemption amount as priced by the financial institution.

3. **Accuracy, Timelines, and Reliability**
   a. **How will data collected from sources other than bureau records be verified for accuracy?**
      All routing (ABA) numbers used by financial institutions are validated using the accepted method published in the *Thomson Key to Routing Numbers.*
      All deposits from valid financial institutions are balanced and adjustments are made back to the financial institution and/or customer to resolve any out-of-balance conditions.

   b. **How will data be checked for completeness**
      The check (last) digit of each routing number is validated using the accepted method published in the *Thomson Key to Routing Numbers.*

The data is searched for any anomalies and "proofed" before being transferred to the Bureau of the Public Debt.

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, the EZ Clear Proof Procedures include a section that shows how to send an encrypted Redemption file (called an ROI File) for processing by BPD each day.

d. **Are the data elements described in detail and documented? If yes, what is the name of the document?**
Yes. The EZ Clear Item Master File Layout document.

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 new data is derived. The Item Master File and associated files are stored on LTO tapes and retained for a rotating 90-day period.

3. **Will the new data be placed in the individual's record?**
N/A – No new data is derived.

4. **Can the system make determinations about employees/public that would not be possible without the new data?**
N/A – No new data is derived.

5. **How will the new data be verified for relevance and accuracy?**
N/A – No new data is derived.

6. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
Data security rules are in place to limit access to the data to FRS employees with valid log-on ids and passwords who are authorized by management to access that data. Semi-annual reviews of the access rights for each employee are conducted. A Continuous Monitoring review for EZ Clear was completed on December 14, 2006.

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

Yes. Data security rules are in place to limit access to the data to FRS employees with valid log-on ids and passwords who are authorized by management to access that data. Semi-annual reviews of the access rights for each employee are conducted.

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.**
   EZ Clear data is mainly retrieved using a savings bond serial number. The data can also be retrieved using an individual's SSN.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
   N/A - EZ Clear does not produce any reports on individuals.

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 main EZ Clear operations are located at the Federal Reserve Bank of Cleveland, Pittsburgh Branch with a Contingency Site located at the Federal Reserve Bank of Cleveland, main office in Cleveland. All updates to the main systems are transferred to the contingency system each week by the Data Center personnel at both sites.

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 and approved by the National Archives and Records Administration (NARA). Paper and microform records ready for disposal are destroyed by 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)?**
   No.

5. **How does the use of this technology affect public/employee privacy?**
   N/A – EZ Clear does not use any technology that would affect privacy.

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 – EZ Clear does not monitor individuals.

8. **What controls will be used to prevent unauthorized monitoring?**
   N/A – EZ Clear does not monitor individuals.

9. **Under which Privacy Act SORN does the system operate? Provide number and name.**
   Treasury/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 and FY07.

Access to Data

1. **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others.)**
   Only FRS employees have access to EZ Clear. Those employees are users, managers, developers, security administrators, and Data Center Personnel.

2. **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
   The FRS management team designates employees who can access EZ Clear and their specific access capabilities. Both FRS and Treasury Retail Security (TRS) Department procedures are used to ensure each employee is assigned the EZ Clear access rights commensurate with his/her job responsibilities.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**
   Users have limited access based on their job responsibilities. Within EZ Clear, there are four levels of access; User, System User, Privilege User, and Security Admin. At the User and System User levels, further access is control by assigning a access menu that only allows access to certain programs. Privilege Users are Data Center personnel and Security Admin are Information Security personnel. An employee's supervisor/manager must authorize all access capabilities before they are submitted to the TRS Department data security contact.

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 employees are required to (electronically) sign the FRS *Rules of Behavior* document, annually.
Data security and valuables handling training sessions are conducted annually for all TRS Department employees.
Semi-annual information security reviews of all EZ Clear access capabilities are completed by TRS Department managers/supervisors.

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 with design and development of the system.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**
   Yes. Various output files are used as input into the Bureau of the Public Debt's SaBRe and RBI systems in Parkersburg, WV.
   Adjustment settlement information is transferred to the FRS's Integrated Accounting (IAS), Ca$hLink systems and to the BPD's Public Debt and Reporting (PARS) system.
   Redemption commission credits for financial institutions are transferred via FRS Automated Clearing House (ACH) system.

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

   All BPD and FRB 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)?**
   EZ Clear does not share data with any other entities outside of the list provided in Question 6.

9. **How will the data be used by the other agency?**
   N/A – See previous answer.

10. **Who is responsible for assuring proper use of the data?**
    All BPD and FRB 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.