SnAP Privacy Impact Assessment (PIA)

September 1, 2007

System Information

Name of System, Project or Program: SnAP
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).**

   Tom Bronder
   Senior Business Analyst, Treasury Retail Securities Department
   Federal Reserve Bank of Cleveland, Pittsburgh Office
   412-261-1469
   tbronder@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? (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 McCoy
   Assistant Commissioner
   Office of Information Technology
   304-480-6635
   kim.mccoy@bpd.treas.gov
   Bureau of the Public Debt
   Parkersburg, WV 26101

System Application/General Information

1. **Does this system contain any information in identifiable form?**
   Yes

2. **What is the purpose of the system/application?**
   Accept savings bond orders and payment authorizations from financial institutions, companies, and government agencies; validate all orders, and produce printed savings bonds and supporting files and documentation**.**

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

Data in the System

1. **What categories of individuals are covered in the system?**
   Entities and United States citizens who purchase or receive United States Savings Bonds.

2. **What are the sources of the information in the system?**
   Individuals, financial institutions, companies, and government agencies provide data to SnAP in electronic and paper form.

   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?**
      Over-the-counter mail-in applications are provided by individuals; however the major source of the data is an individual's financial institution, an individual's employer, or a company an individual does business with.

   b. **What Federal agencies are providing data for use in the system?**
      Various Federal agencies throughout the country provide input for use in the system.

   c. **What State and/or local agencies are providing data for use in the system?**
      Various Federal agencies throughout the country provide input for use in the system.

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

Data is provided to SnAP by financial institutions, companies, and government agencies.

e. What information will be collected from the employee and the public?
Employees of the FRS can participate in the savings bond deduction program. Each of those FRS employees must provide their SSN, name, a valid mailing address, and, optionally a second named owner of the savings bond. Other companies and government agencies that participate in savings bond deduction programs collect similar information from their employees. Financial institutions collect the same information from their customers.

3. Accuracy, Timelines, and Reliability

a. How will data collected from sources other than bureau records be verified for accuracy?
Each company, government agency, and financial institution is assigned a "company identifier" in SnAP. Only orders with valid "company identifiers" are processed.
All routing (ABA) numbers used by financial institutions are validated using the accepted method published in the *Thomson Key to Routing Numbers.*
The SSN/TIN/EIN of all bond owners is validated using rules provided by the SSA. All city, state and zip codes are verified using third party software (Group One).

b. How will data be checked for completeness
Each company identifier is matched to the SnAP customer table.
The check (last) digit of each routing number is validated using the accepted method published in the *Thomson Key to Routing Numbers.*
The SSN/TIN/EIN of all bond owners is validated using rules provided by the SSA.
All city, state and zip codes are verified using third party software (Group One).

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.)
Each company identifier is matched to the SnAP customer table.
The check (last) digit of each routing number is validated using the accepted method published in the *Thomson Key to Routing Numbers.*
The SSN/TIN/EIN of all bond owners is validated using rules provided by the SSA.
All city, state and zip codes are verified using third party software (Group One) that is updated twice a year.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?
Yes. The *SnAP Data Dictionary Report (SnAP136U)* identifies the attributes of the data elements.

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?**
   Yes. A database of all completed transactions and issued savings bonds is compiled and stored on SQL servers. The data is maintained for 12 calendar months, and then it is replaced by similar data for the current year. No data is derived.

3. **Will the new data be placed in the individual's record?**
   No.

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

5. **How will the new data be verified for relevance and accuracy?**
   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. The latest review was completed on April 17, 2007. A Continuous Monitoring review for SnAP was completed on April 27, 2007.

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.**
   SnAP data is usually retrieved using a person's SSN. The data can also be retrieved using the bond owner's last name, the FRS assigned company identifier or the SnAP assigned transaction identifier.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
   Internal FRS reports can be produced to summarize all data that has been aggregated. Those reports are used to verify data provided by companies, government agencies, and financial institutions. Only FRS employees with data security access privileges can generate those 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?**
   SnAP systems are installed at FRB Minneapolis and FRB Pittsburgh. All updates are made concurrently to both systems by one group of developers and one group of database administrators.

2. **What are the retention periods of data in this system?**
   The retention period for SnAP data is six (6) months.

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 six (6) months, the automated back-up system marks the SnAP data as "deleted." The physical magnetic media is made available for reuse. All back-ups are performed by the Information Technology Department according to their department procedures. All SnAP reports are maintained in an archive.

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 – See previous answer.

6. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
   Yes. SnAP does maintain the SSN, name, and address to identify savings bond customers. SnAP is not capable of locating or monitoring any individual.

7. **What kinds of information are collected as a function of the monitoring of individuals?**
   N/A – SnAP does not monitor individuals.

8. **What controls will be used to prevent unauthorized monitoring?**
   N/A – SnAP 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/

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 SnAP. Those employees are users, managers, developers, and data base administrators.

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 SnAP and their specific access capabilities. Both FRS and Treasury Retail Security (TRS) Department procedures are used to ensure each employee is assigned the SnAP 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 SnAP, there are 123 data security functions. Each of those functions permits a user to access a specific SnAP menu option. 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 FRB Pittsburgh employees are required to (electronically) sign the FRS *Rules of Behavior* document, annually.

All FRB Minneapolis employees are required to adhere to their Information Security Use of Bank Equipment and Services Policy.
Data security and valuables handling training sessions are conducted annually for all TRS Department employees.
Information security reviews of all SnAP access capabilities are completed by TRS Department managers/supervisors at least twice each year..

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.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**
   Yes. Interface files are shared by SnAP with other FRS controlled systems.
   Savings bond order files are accepted from the Savings Bond Direct (SBD, on the TWAI), the Automated Book Entry (ABE), and the Savings Bond Redemption (SABRS) systems.
   Daily proof data is received from ABE, SABRS, the Vault Management (VMS), and Tracking and Control (TCS) systems.
   Settlement information is transferred to the FRS' Integrated Accounting (IAS), Automated Clearing House (ACH), and Ca$hLink systems; and to the BPD owned Public Debt and Reporting (PARS) 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)?**
   Other than the entities noted in (6) above, the answer is No.

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.