SnAP Privacy Impact Assessment (PIA)

September 1, 2008

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).**

   Walter J. Patsilevas
   Business Analyst, Treasury Retail Securities Department
   Federal Reserve Bank of Cleveland, Pittsburgh Office
   412-261-7709
   wpatsilevas@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
   Bureau of the Public Debt
   Parkersburg, WV 26101

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 Security Officer
   Office of Information Technology
   (304) 480-7972
   jim.mclaughlin@bpd.treas.gov
   Bureau of the Public Debt
   Parkersburg, WV 26101

5. **Who is the Bureau Privacy Act Officer who reviewed this document? (Name, title, organization, phone, email, address).**

   Denise Nelson
   Disclosure Officer
   Office of Management Services
   (304) 480-8402
   denise.nelson@bpd.treas.gov
   Bureau of the Public Debt
   Parkersburg, WV 26101

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.mcoy@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?**

   Bureau of the Public Debt
   Parkersburg, WV 26101

4. **Under which Privacy Act SORN does the system operate? (Provide the system name and unique system identifier.)**

   The SORN (statement of records notification) for saving securities is BPD.002- United States Savings - Type Securities. The most current copy of the SORN notification is attached. It was published in the Federal Register/Vol 73 , No. 142/ July 23, 2008/ notices.

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 State and local 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 and companies throughout the country.

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

   - Companies and government agencies that participate in savings bond deduction programs collect the employees SSN, name, a valid mailing address and optionally a second named owner of the savings bond.
   - Financial Intuitions collect the same information from customers who purchases savings bonds.
   - The public submits registration information directly to the Federal Reserve when sending in "mail-ins" to the Over-the-Counter operation. This registration information includes SSN, name, mailing address, and optionally a second named owner of the savings bond.

3. **Accuracy, Timelines, and Reliability**
    a. **How will data collected from sources other than bureau records are 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. Critical data elements (Company Identifier, order and effective payment dates, and dollar amounts) are dual passed and balanced by separate operators. The SnAP and department proofs are balanced prior to the printing of the Savings bonds.
        - 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 Social Security Administration. 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 Social Security Administration. 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 Social Security Administration. 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?**

   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 16, 2008.
   - SnAP is a FISMA-compliant application. A full FISMA review was completed in April 2008 and a Delta C&A was completed in June 2008 due to the installation of new servers.

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. All changes must go through a change control process that includes approval by management and data security administrators.

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

   The retention period for SnAP data is twelve (12) 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?**

   SnAP does not use any technologies that the bureau/office has not previously employed. Safeguards are in place to allow users in the SnAP system to only have access to data that they need to perform their jobs.

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?**

   SnAP does not monitor individuals.

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

   SnAP does not monitor individuals.

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

   The SORN (statement of records notification) for saving securities is BPD.002- United States Savings - Type Securities. The most current copy of the SORN notification is attached. It was published in the Federal Register/Vol 73 , No. 142/ July 23, 2008/ notices.

10. **If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.**

    The system is not being revised so no update to the SORN is required

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. In addition, temporary agency employees have limited access to data during seasonal processing periods.

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 128 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?**

Amy J. Heinl
Vice President
Federal Reserve Bank of Cleveland, Pittsburgh Office
412-261-1446
Amy.J.Heinl@clev.frb.org
717 Grant Street
Pittsburgh, PA 15219

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?**

Data is not used by other agencies.

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

Amy J. Heinl
Vice President
Federal Reserve Bank of Cleveland, Pittsburgh Office
412-261-1446
Amy.J.Heinl@clev.frb.org
717 Grant Street
Pittsburgh, PA 15219