



**Savings Bond Architecture Platform (SnAP)
Privacy Impact Assessment (PIA)**

January 15, 2010

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).**

Leigh Anne Kustra
Business Analyst, Treasury Retail Securities
Federal Reserve Bank of Cleveland, Pittsburgh Branch
412-261-7456
Leigh.A.Kustra@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
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 Branch
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 D. McLaughlin
Chief Information Security Officer / Privacy Act Officer
Office of Information Technology
Security Program Staff
304-480-6635
Jim.McLaughlin@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
304-480-6635
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?

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.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.)

The SORN (statement of records notification) for saving securities is BPD.002- United States Savings - Type Securities.

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 with whom an individual does business.

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 employee's social security number (SSN), name, a valid mailing address and optionally a second named owner or beneficiary of the savings bond.
- Financial Institutions collect the same information from customers who purchase savings bonds.
- The public submits registration information directly to the Federal Reserve Bank when sending in "mail-ins" to the Over-the-Counter operation. This registration information includes SSN, name, mailing address, and a second named owner or beneficiary of the savings bond (optional).

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. 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 *ABA 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.

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.

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 *ABA 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 (Satori) that is updated bi-monthly.

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 new 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 March 18, 2009.
- 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. The most recent Continuous Monitoring was completed in July 2009.

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 programming 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 in the SnAP System is twelve (12) months for CBT data. The retention period for Work in Process data is 4 1/2 months and for Print data is 2 1/2 weeks.

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?

Data are deleted based on retention time parameters by a SnAP delete program written per SnAP business rules. Data are backed up to a backup medium and stored for a period of 62 days. The physical magnetic media can be made available for reuse/restores. All back-ups are performed by the Information Technology Department according to their department procedures. All SnAP reports are maintained in the SnAP archive system on the SnAP server. Procedures are documented in the ITS Standards and Procedures database.

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.

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

These records may be disclosed to:

- Agents for 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 bonds registered in that form or to the beneficiary for bonds 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 statute, 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 owing debts to the BPD to other Federal agencies for the purpose of determining whether the debtor is a Federal employee or retiree receiving payments which may be used to collect the debt through administrative or salary offset
- Disclose through computer matching information on holdings of savings-type securities to requesting Federal agencies under approved agreements limiting the information to that which is relevant in making a

determination of eligibility for Federal benefits administered by those agencies

- 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 matured, unredeemed 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

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 127 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 Bonds Direct (SBD, on the TWAI) and the Savings Bond Redemption (SABRS) systems.
- Daily proof data is received from 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 Accounting 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. Heintl
Vice President
Federal Reserve Bank of Cleveland, Pittsburgh Branch
412-261-1446
Amy.J.Heintl@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. Heidl
Vice President
Federal Reserve Bank of Cleveland, Pittsburgh Branch
412-261-1446
Amy.J.Heidl@clev.frb.org
717 Grant Street
Pittsburgh, PA 15219