



**Savings Bond Redemption System (SaBRS)
Privacy Impact Assessment (PIA)**

9/26/2012

System Information

Name of System, Project or Program: Savings Bond Redemption System (SaBRS)

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).**

Dana Keeley
Business Analyst
Treasury Retail Securities
Federal Reserve Bank of Minneapolis
800-553-2663
Dana.Keeley@mpls.frb.org
90 Hennepin Ave.
Minneapolis, MN 55401

- 2. Who is the system owner? (Authorizing Official Name, title, organization, phone, email, address).**

Paul V. Crowe
Assistant Commissioner
Office of Retail Securities
Bureau of the Public Debt
304-480-6516
Paul.Crowe@bpd.treas.gov
200 Third Street, Room 501
Parkersburg, WV 26106-1328

- 3. Who is the system manager? (Name, title, organization, phone, email, address).**

Brian Duncan
Manager
Treasury Retail Securities
Federal Reserve Bank of Minneapolis
800-553-2663
Brian.Duncan@mpls.frb.org
90 Hennepin Ave.
Minneapolis, MN 55401

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

David Ambrose
Chief Information Security Officer
Privacy Officer
Financial Management Service &
Bureau of the Public Debt
202-874-6488
David.Ambrose@fms.treas.gov
3700 East-West Highway
Hyattsville, MD 20782

5. Who is the IT Reviewing Official? (CIO Name, title, organization, phone, email, address).

Kimberly A. McCoy
Chief Information Officer
Assistant Commissioner
Office of Information Technology
Bureau of the Public Debt
304-480-6988
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?

SaBRS provides the following Savings Bonds functionality: redemptions, full/partial refunds of purchase price, payments, taxable reissues, bond pricing only, tax record creation storage and transmission, and payment functions.

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.)

BPD.002—United States Savings-Type Securities
BPD.003—United States Securities (Other than Savings-Type Securities)
BPD.008—Retail Treasury Securities Access Application
BPD.009—U.S. Treasury Securities Fraud Information System.

Data in the System

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

Owners of U.S. savings securities.

2. What are the sources of the information in the system?

The sources of information in the system include redemptions and other requests from customers (individuals, financial institutions).

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?

Individuals complete appropriate request documentation for savings securities redemptions. Requests are submitted by the individual or by a financial institution on behalf of an individual.

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

The Bureau of Public Debt provides redemption tables used to calculate redemption values in the system.

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 following information is collected for redemption requests: Social Security Number, name, mailing address, bank account information (only for those customers requesting ACH payment).

3. Accuracy, Timelines, and Reliability

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

- Critical data elements are dual passed and balanced by separate operators.
- A proof process is completed before payments are issued.
- 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.

b. How will data be checked for completeness

Information submitted by the bond owner is manually reviewed for completeness. In addition, validation of certain key data elements including SSN/TIN/EIN and routing numbers is completed.

- 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.)**

Information submitted by the bond owner is current. Validation of certain key data elements including SSN/TIN/EIN and routing numbers is completed to ensure data is current.

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

Yes. Data elements are described in the SaBRS System Documentation Section III – SQL Database Structure 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 not derived.

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

N/A

- 4. Can the system make determinations about employees/public that would not be possible without the new data?**

N/A

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

N/A

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

Data is consolidated to for the IRS 1099 and 1042. Logical access restrictions are in place to prevent unauthorized use and ensure only those with a need to know can access the information.

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

N/A – process are not being consolidated.

- 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 by searching the following key data elements: SSN/TIN/EIN, payee name, transaction ID, tracking number, and ABA (if applicable). SSN/TIN/EIN is a personal 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?**

The IRS 1099 and 1042 are the only reports produced for an individual. The reports are used for reporting redemptions to the IRS.

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?**

There are two separate instances of SaBRS. One is operated at FRB Minneapolis and the other is operated at the Bureau of Public Debt (BPD). This Privacy Impact Assessment (PIA) is limited to the instance in operation at FRB Minneapolis.

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

SaBRS application and database records are retained for 6 years, 3 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?**

Data are manually purged periodically based on retention time parameters. Electronic backups (server to server) of the SaBRS system data are completed daily. The data is backed-up from the SaBRS server to a designated server at the FRB Minneapolis contingency site. All back-ups are performed by the Information Technology Department according to their department procedures. Treasury Retail Securities staff is responsible for obtaining the proper approvals prior to destruction of data produced from the application.

- 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?**

SaBRS does not use any technologies that the bureau/office has not previously employed. Safeguards are in place to allow users in the SaBRS system to only have access to data that they need to perform their jobs. Information about employees is not stored in this system.

- 6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
SaBRS provides the capability to identify and locate an individual. SaBRS maintains the SSN, name, and mailing address to identify savings bond customers. SaBRS does not have the capability to monitor individuals.
- 7. What kinds of information are collected as a function of the monitoring of individuals?**
N/A - SaBRS does not monitor individuals.
- 8. What controls will be used to prevent unauthorized monitoring?**
N/A - SaBRS 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 modified.

Access to Data

- 1. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others.)**
Only the Federal Reserve System (FRS) employees have access to SaBRS. Those employees are users, managers, developers, and database administrators.
- 2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
Access is driven by the role of the user and their position as it relates to the Retail Securities business. Procedures are in place to manage the access process whereby the Treasury Retail Securities management staff authorize/request access for individuals.
- 3. Will users have access to all data on the system or will the user's access be restricted? Explain.**
The system employs a role-based access model. Staff is placed in groups according to the business need.
- 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.)**

- a. All FRB Minneapolis employees are required to adhere to their Information Security Policy.
 - b. Data security and valuables handling training sessions are conducted annually for all Treasury Retail Security (TRS) Department and Public Debt employees.
 - c. All TRS employees completed an on-line training course to comply with the “Sensitive But Unclassified” mandate for Federal Reserve Banks.
 - d. All TRS employees completed the annual *Information Security: Security Matters* and *Treasury Privacy Matters* on-line training courses.
 - e. Users follow Rules of Behavior
 - f. FRB Minneapolis personnel are subject to background investigations and periodic re-investigations as a condition of employment.
 - g. Other mitigating controls include Security Assessment and Authorization, and Continuous Monitoring.
- 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 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 - Interface files are shared by SaBRS with other FRS controlled systems. Settlement information is transferred to the FRS Integrated Accounting System (IAS) and Automated Clearing House (ACH). In addition, FRB Philadelphia prints and mails IRS 1099s and 1042s.
- 7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
All employees with access to the system or data produced by the system are responsible for protecting the privacy rights of the public.
- 8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?**
The IRS will receive reports (IRS 1099 and 1042) from the system.
- 9. How will the data be used by the other agency?**
The IRS will use the IRS 1099s and 1042s for tax purposes.
- 10. Who is responsible for assuring proper use of the data?**
All employees with access to the system or data produced by the system are responsible for assuring proper use of the data in accordance with information classification and handling policies.

Attach Signature Page