The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service Privacy Impact Assessments (PIA):
https://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Treasury Retail Securities Software Applications (TRSSA)

Document Version: 2

Document Date: 7/21/2016

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

TRSSA is comprised of applications that support Savings Bonds operations. These applications are the Savings Bond Architectural Program (SnAP), Savings Bond Replacement System (SaBRS), and Vault Management System (VMS).

SnAP

SnAP accepts savings bond orders and payment authorizations from companies and government agencies, validates all orders, produces files to send to the print site, and produces supporting files and documentation. SnAP also holds records for electronic book entry units.

SaBRS

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

VMS

The VMS application is used to track and account for uninscribed bond stock held by Treasury Services. VMS will be omitted in this document since this component does not contain Personally Identifiable Information (PII) of any kind.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

- 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.

3) If the system is being modified, will the SORN require amendment or revision?

__yes, explain.
_X_no

4) Does this system contain any personal information about individuals?
_X_yes
__no

a. Is the information about members of the public?

Yes

b. Is the information about employees or contractors?

Yes

5) What legal authority authorizes the purchase or development of this system?

Bureau of the Fiscal Service
Parkersburg, WV 26101

5 U.S.C. §301; 31 U.SC. §3101, *et seq*

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Entities and United States citizens who purchase or receive United States Savings Bonds.

Check all that apply:
_X_ Employees
_X_ Contractors
_X_ Taxpayers
__ Others (describe)

2) Identify the sources of information in the system
Check all that apply:
_X_ Employee
_X_ Public
_X_ Federal agencies (FS systems TRES Siebel, TreasuryDirect, Legacy Treasury Direct, HH/H System)
__ State and local agencies
_X_ Third party

a. What information will be collected from employees or contractors?

If an employee redeems/reissues a savings bond or requests to purchase a savings bond the following information is collected: Tax Identification Number (e.g., Social Security Number or Employer Identification Number), name, mailing address, bank account information if requesting ACH payment, and a second named owner or beneficiary of the savings bond if applicable.

b. What information will be collected from the public?

SaBRS

The following information is collected for redemption requests: Tax Identification Number (e.g., Social Security Number or Employer Identification Number), name, mailing address, and bank account information for customers requesting ACH payment.

SnAP

- The Internal Revenue Service (IRS) collects information from customers who purchase savings bonds with tax refund monies. This information is Tax Identification Number (TIN), name, mailing address, and a second named owner or beneficiary of the savings bond if applicable.
- Companies send in requests to purchase units (no PII).
- The public submits registration information directly to the Federal Reserve Bank when sending corrections to Tax Time Bonds. This registration information is TIN, name, mailing address, and a second named owner or beneficiary of the savings bond if applicable.

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

SaBRS

Fiscal Service provides redemption tables used to calculate redemption values in the system.

SnAP

Fiscal Service provides redemption tables used to calculate redemption values in the system. Additionally, IRS sends electronic files for savings bonds purchased with tax refund monies.

d. What state and local agencies are providing data for use in the system?

SaBRS

None

SnAP

None

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

SaBRS

None

SnAP

Companies participating in the Book Entry program

3) Accuracy, Timeliness, and Reliability

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

SaBRS

- Critical data entry elements are first passed, second 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 TIN of all bond owners is validated using rules provided by the Social Security Administration.

SnAP

- Each company and government agency is assigned an "identifier" in SnAP. Only orders with valid "identifiers" are processed. Critical data entry elements (identifier, order and effective payment dates, and dollar amounts) are first passed, second passed, and balanced by separate operators. The SnAP and department proofs are balanced prior to sending the print file to the print site.
- All routing (ABA) numbers used by government agencies are validated using the accepted method published in the *ABA Key to Routing Numbers.*

- The TIN of all bond owners is validated using rules provided by the Social Security Administration.

- All city, state, and ZIP code entries are verified using third party software.

b. How will data be checked for completeness?

SaBRS

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

SnAP

- Each 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 TIN of all bond owners is validated using rules provided by the Social Security Administration.

- All city, state and ZIP code entries are verified using third party software.

c. What steps or procedures are taken to ensure the data is current?

SaBRS

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

SnAP

- Each 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 TIN of all bond owners is validated using rules provided by the Social Security Administration.

- All city, state and ZIP code entries are verified using third party software that is updated bi-monthly.

d. In what document(s) are the data elements described in detail?

SaBRS

Data elements are described in the SaBRS System Documentation Section III – SQL Database Structure document.

SnAP

The SnAP Data Dictionary Report (SnAP136U) identifies the attributes of the data elements.

ATTRIBUTES OF THE DATA:

1) **How is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

SaBRS

The use of data captured is necessary to process savings bond redemption requests from investors. Payment is issued to the investor after processing is complete. Tax information for IRS Form 1099 is also sent annually.

SnAP

The use of data captured is necessary to process savings bond issues and reissues from investors. Currently, investors can purchase Tax Time bonds as paper bonds.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?**

SaBRS

No – new data is not derived.

SnAP

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 or members of the 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 security rules are in place to limit access to the data to Federal Reserve System (FRS) employees who have valid log-on IDs and passwords, and who are authorized by management to access that data. Semi-annual reviews of the access rights for each employee are conducted.

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

N/A – processes are not being consolidated.

8) How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)

SaBRS

Data can be retrieved by searching the following key data elements: TIN, payee name, transaction ID, tracking number, and, if applicable, an ABA routing number. TIN is a personal identifier.

SnAP

SnAP data is usually retrieved using a TIN. 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 kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

SaBRS

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

SnAP

Internal FRS reports can be produced to summarize all data that has been aggregated. Those reports are used to verify data provided by companies and government agencies. Only FRS employees with data security access privileges can generate those reports.

10) What opportunities do individuals have to decline to provide information (i.e., in such cases where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)? How can individuals grant consent?

All information gathered from the customer is voluntary. If a customer prefers not to provide the requested information, positive identification may not be possible. In such a case, the customer may provide a written request.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) What are the retention periods of data in this system? How long will the reports produced be kept?

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 according to their respective retention schedules.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?

SaBRS

Data is manually purged periodically based on retention time parameters. Electronic backups (server to server) of the SaBRS system data is completed daily. The data is backed up from the SaBRS server to a designated server at the Federal Reserve Bank (FRB) contingency site. All back-ups are performed by the Information Technology Department according to its department procedures. Treasury Retail Securities staff is responsible for obtaining the proper approvals prior to destruction of data produced from the application in accordance with the File Plan. Staff that are responsible for disposition of the data maintain the procedures within their respective department.

SnAP

Data is deleted based on retention time parameters by a SnAP delete program written per SnAP business rules. Electronic backups (server to server) of the

SnAP system data are completed daily. The data is backed up from the SnAP server to a designated server at the FRB contingency site. All back-ups are performed by the Information Technology Department according to its 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. IRS bond data is stored per IRS requirements in a separate SnAP Data Warehousing database.

3) If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?

SaBRS

There are two separate instances of SaBRS. One is operated at the FRB and the other is operated at Fiscal Service. This Privacy Impact Assessment is limited to the instance in operation at the FRB.

SnAP

SnAP is operated at FRB– there is only one site.

4) Is the system using technologies in ways that Fiscal Service has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect employee or public privacy?

SaBRS

SaBRS does not use any technologies that the bureau 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.

SnAP

SnAP does not use any technologies that the bureau 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.

SaBRS and SnAP

SaBRS and SnAP provide the capability to identify and locate an individual. Both maintain the TIN, name, and mailing address to identify savings bond customers. Neither application has the capability to monitor individuals.

7) What kind of information is collected as a function of the monitoring of individuals?

N/A - TRSSA does not monitor individuals.

8) What controls will be used to prevent unauthorized monitoring?

N/A - TRSSA does not monitor individuals.

ACCESS TO DATA:

1) Who will have access to the data in the system?
Check all that apply:

__ Contractors
_X_ Users
_X_ Managers
_X_ System Administrators
_X_ System Developers
__ Others (explain)_____

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 his or her 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 request and authorize access for individuals.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

SaBRS

The system employs a role-based access model. Staff is placed in groups according to the business need.

SnAP

Users have limited access based on their job responsibilities. Within SnAP, there are 130 data security functions. Each of those functions permits a user to access a specific SnAP menu option. An employee's supervisor or manager must authorize any capabilities in an access request before it is 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? (Please list processes and training materials)

- All FRB employees are required to adhere to their Information Security Policy.
- Training sessions for data security and valuables handling are conducted annually for all TRS Department employees.
- Information security reviews of all access capabilities are completed by TRS Department managers or supervisors at least twice each year.
- Security Assessment and Authorization (SA&A) review is completed annually, and continuous monitoring is in place.

5) If contractors are or will be involved with the design, development or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?

SaBRS and SnAP

No contractors are involved with the design and development of the systems.

6) Do other systems share data or have access to the data in the system?

SaBRS

_X_yes
__no

SnAP

_X_yes
__no

If yes,

A. Explain the interface.

SaBRS

Interface files are shared by SaBRS with other FRS and Fiscal Service controlled systems. Settlement information is transferred to the SnAP application and Retail Accounting and Payments System (APA). In addition, Fiscal Service prints IRS Form 1099 and 1042.

SnAP

- Interface files are shared by SnAP with other FRS controlled systems.
- Daily proof data is received from SABRS.
- Settlement information is transferred to the FRS EASy and Direct Voucher Submission (DVS) systems, and to the Fiscal Service-owned Summary Debt Accounting System (SDAS) System.

b. Identify the role 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. Employees affected by the interface are protected in accordance with information classification and handling policies.

7) Will other agencies share data or have access to the data in this system?

_X_yes
__no

If yes,

a. Check all that apply:

_X_Federal
__State
__ Local
__Other (explain) _____

b. Explain how the data will be used by the other agencies.

SaBRS

The IRS will receive reports (IRS Form 1099 and 1042) from the system.

SnAP

For accounting purposes, settlement information is transferred to the FRS EASy and DVS systems and to the Fiscal Service-owned Summary Debt Accounting System (SDAS) system.

c. Identify the role 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.