



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://fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Series HH/H Savings Bond System (HH/H)

Document Version: 2.0

Document Date: March 6, 2018

SYSTEM GENERAL INFORMATION:

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

The HH/H system is classified as a major application and provides processing required to establish, maintain, report, and service bondholder accounts relative to series F, G, H, HH, J, and K current income savings bond activity.

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.009 - U.S. Treasury Securities Fraud Info. System

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

No.

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

Yes.

a. Is the information about members of the public?

Yes.

b. Is the information about employees or contractors?

No.

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

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

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Check all that apply:

- Employees
- Contractors
- Taxpayers
- Others (describe)

2) Identify the sources of information in the system.

Check all that apply:

- Employee
- Public
- Federal agencies
- State and local agencies
- Third party

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

None.

b. What information will be collected from the public?

The following information is collected from customers to process reissuances, holdings, transactions, claims, and inquiries:

- Name of registered owner, or Co-Owner(s), or Beneficiary
- TIN of the registered owner, or Co-Owner(s), or Beneficiary
- Inscription address
- Bank Information
- Collect legal information such as trust information, estate information, guardianship information.

Holdings: Records documenting ownership, status, inscription information, payment activity, non-receipt or over- or underpayments of interest and principal, and numerical registers of ownership.

Transactions (redemptions, payments, and reissues): Records, which include securities transaction requests, interest activity, legal papers supporting transactions, applications for disposition or payment of securities and/or interest thereon of deceased or incapacitated owners, records of retired securities, and payment records.

Claims: Records including correspondence concerning lost, stolen, destroyed, or mutilated savings-type securities; bonds of indemnity; legal documents supporting claims for relief; and records of caveats entered.

Inquiries: Records of correspondence with individuals who have requested information concerning current income securities, redemption of said securities, and/or interest thereon.

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

None.

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

None.

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

None.

3) Accuracy, Timeliness, and Reliability

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

The certifying officer must require the person presenting a bond, or appropriate Fiscal Service transaction form, to establish his or her identity in accordance with Department of Treasury instructions and identification guidelines.

b. How will data be checked for completeness?

The HH/H system will edit specific fields to see that the data has the correct type and number characters and is in the correct format.

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

Processing errors in the system involving incorrect information are handled quickly. When account holders call customer service, key data elements are reviewed with the customer and fields are updated as needed.

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

Data elements are described in detail and documented in the E-Source Guides with cross-references to the Federal Register, Department Circular (Treasury), and Code of Federal Regulations. The HH/H interface document in the Production Operating Procedures manual lists required data elements, descriptions, field type, and sizes.

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?

Information in this system of records is collected and maintained to enable Fiscal Service and its agents to process transactions, to make payment, and to identify owners and their accounts.

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?

No.

3) Will the new data be placed in the individual's record?

Not applicable.

4) Can the system make determinations about employees or members of the public that would not be possible without the new data?

Not applicable.

5) How will the new data be verified for relevance and accuracy?

Not applicable.

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

Data is not being consolidated within the HH/H system.

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

The system possesses multiple layers of protection for the personal information contained. This infrastructure utilizes perimeter security firewalls, access control lists, and secure communications.

All Fiscal Service employees are required to take annual training on the security and protection of PII.

The application employs the principle of least privilege, allowing only authorized accesses that further protect the databases containing this information. All operational support personnel receive and acknowledge rules of behavior that provide instructions regarding protection of personal information.

Management controls supplement logical and physical protections by requiring regular and frequent review of audit trails, audit logs, and access violation reports. Fiscal Service's computing infrastructure is subject to frequent independent audits and regular security reviews.

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.)

Data can be retrieved in a number of ways using a personal identifier. Information can be retrieved alphabetically by name, address, by bond serial numbers, other assigned identifier, or, in some cases, numerically by taxpayer identification number (social security number or employer identification number). In the case of securities registered in more than one name, information relating thereto can be retrieved only by the names,

or, in some cases, the taxpayer identification number of the registrants, primarily the registered owners or first-named co-owners. In the case of gift bonds inscribed with the taxpayer identification number of the purchaser, bonds are retrieved under that number or by bond serial number.

9) What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Most system reports are generated for accounting and audit verification of transactions processed in the system. Account history and security history are maintained within the system. Accounting and customer service personnel have capabilities to access the 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?

Fiscal Service forms that customers are requested to complete include Privacy Act language which asserts the furnishing of information is voluntary, however, without the information the Fiscal Service may be unable to process transactions.

By completing and signing the forms, customers are granting consent.

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 otherwise until they are no longer historically significant.

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

Other records are disposed of at varying intervals in accordance with records retention schedules reviewed, approved, and documented by the National Archives and Records Administration (NARA). Paper and microform records that are ready for disposal are destroyed by shredding or maceration. Records in electronic media are electronically erased using accepted techniques.

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?

The system is maintained at a Fiscal Service facility. Fiscal Service uses remote copy technology for data replication to our backup facility.

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?

The HH/H system does not use any technologies that the Bureau/Office has not previously employed. Safeguards are in place to allow users of the HH/H system to only have access to the data they need to perform their job duties. The public does not have access to the HH/H system.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes. Information in this system of records is collected and maintained to enable Fiscal Service and its agents to process transactions, make payments, and identify owners and their accounts.

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

Information in this system of records is collected and maintained to enable Fiscal Service to process transactions, make payments, and identify owners and their accounts. Information collected includes: name of registered owner or first named co-owner, TIN of the registered owner or first named co-owner, name of beneficiary or second named co-owner, TIN of the beneficiary or second named co-owner, and inscription address.

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

Information is contained in secure buildings, or in areas which are occupied either by officers and responsible employees or agents of Fiscal Service who are required to maintain proper control over records while in their custody. These officers and responsible employees are subject to personnel screening procedures and to the Treasury Department Code of Conduct. Additionally, since in most cases numerous steps are involved in the retrieval process, an unauthorized person would be unable to retrieve information in meaningful form. Information stored in electronic media is safeguarded by automatic data processing security procedures in addition to physical security measures. Additionally, for those categories of records stored in computers with online terminal access, the information cannot be accessed without proper passwords and preauthorized functional capability.

ACCESS TO DATA:

1) Who will have access to the data in the system?

Check all that apply:

Contractors

Users _____

Managers

System Administrators

System Developers

✓ Others (explain):

The primary users of data in the system are

- Fiscal Service employees
- Federal Reserve Bank

These records may be disclosed to:

- Agents or 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
- Information provided to trustees, admins of estates, legal guardians, upon submission of the legal documentation that supports the request.
- 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 Department of Veterans Affairs and selected veterans' publications for the purpose of locating owners or other persons entitled to undeliverable bonds held in safekeeping by the Department of the Treasury
- 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

These records may also be:

- Disclosed through computer matching; including information on individuals

owing debts to the Fiscal Service; disclosed 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

- Disclosed through computer matching; including information on holdings of Treasury securities; disclosed 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
- Disclosed through computer matching; including information on individuals with whom the Bureau of the Fiscal Service has lost contact; disclosed to other Federal agencies for the purpose of utilizing letter-forwarding services to advise these individuals to initiate contact the Bureau about returned payments and/or matured, unredeemed securities
- Disclosed to consumer reporting agencies to encourage repayment of an overdue debt. 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.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to the data follows the principles of least privilege and need to know. The system uses role-based access to ensure employees can only process and view data needed to complete their jobs. Separation of duty is enforced to ensure no individual has access to perform both entry and approval within the system.

Fiscal Service maintains documented procedures concerning controls and responsibilities regarding access.

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

User access is restricted. Safeguards are in place to only allow users of the system to have access to the data they need to perform their job duties.

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.)

- Security Plan
- Risk Management Plan
- System Assessment and Authorization process
- Security Matrix
- Rules of Behavior
- Checks and balances through role-based access
- Audit trails/logs
- Continuous Monitoring process

- 5) **If contractors are/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?**

Contractors are not involved with the maintenance of the system.

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

Yes.

If yes,

- a. Explain the interface.**

The system provides the following files:

- Accounting files to the Fiscal Service Accounting and Payments Application (APA)
- Payment files to APA
- Matured unredeemed security files to Treasury Hunt.

The system receives the following files:

- Classified issue and retirement transactions from the classification process.
- Return payment files from APA.

- b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.**

All Fiscal Service 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 Fiscal Service Chief Information Officer (CIO) have the responsibility to see that the data is protected from all threats.

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

Yes.

If yes,

- a. Check all that apply:**

Federal

State

Local

Other (explain) _____

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

Please reference disclosures listed in Section 1.

c. Identify the role responsible for assuring proper use of the data.

All Fiscal Service employees who have access to the system, the system manager, system owner, and ultimately the Fiscal Service Chief Information Officer are responsible for assuring the proper use of data in the system.