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: TreasuryDirect (TD)

Document Version: 2.2

Document Date: November 15, 2016

SYSTEM GENERAL INFORMATION:

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

The TreasuryDirect system is an Internet-based application that enables customers to open an account, buy eligible U.S. Treasury obligations, and manage their accounts and security holdings. The system provides customers with a secure way of viewing and managing all of their Treasury security holdings online with minimal customer service assistance. Currently, the system provides full servicing of electronic U.S. Savings Bonds (Series E, EE, and I), Zero-Percent Certificates of Indebtedness (C of I), and U.S. Treasury marketable securities.

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?

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?

Yes

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?

Employees and contractors may own definitive accrual, current-income, and retirement-type savings securities. The same information will be collected from employees and contractors as is collected from the public. See Section b below for a detailed listing of the information collected.

b. What information will be collected from the public?

The TreasuryDirect application collects the following:

- Account holder's Name,
  - first name (required)
  - middle name or initial (optional)
  - last name (required)
  - suffix (optional); and
  - entity name (entity account only)
- Names of other parties, which include:
  - first name (required)
  - middle name or initial (optional)
  - last name (required); and
  - suffix (optional)
- The other parties are:
  a) secondary owners
  b) beneficial owners
  c) minor children for whose benefit minor linked accounts are established; owner(s) of gift securities purchased or converted by the account-holder
  d) account manager for entity account
- Account-holder's Taxpayer Identification Number (TIN) (required)
- The TIN of other parties (see above definition) - (required)
- Account-holder's email address (required)
- Account-holder's home telephone number (required)
- Account-holder's home address (required), which includes:
  - Full street address
  - City

    - State; and
    - Zip Code
- Account holder's IRS control number (required if establishing an entity account).
- Account-holder's driver's license or state identity card information, which includes:
    - License/Identification number
    - Issuing state
    - Expiration date
- Account-holder's alternate telephone numbers, such as work and cell phone numbers (optional)
- Account-holder's bank information (required), which includes the:
    - Name of the financial institution
    - Account number
    - Financial institution's ABA routing number
    - Names on the bank account; and
    - Bank account type (checking or savings)
- TreasuryDirect Account Number (required).
- Password Hint: a line of text to remind the account-holder of his/her password (required).
- Authentication Questions and Answers: responses to three of ten standardized questions (required).
- Account-holder's date of birth (required).
- Minor child's date of birth (required if establishing a minor account).
- Security registration (required): includes type of registration and owner(s)' full name(s).
- Wire transfer instructions including:
    - Routing Number – ABA: the identification number of the financial institution receiving the security
    - Financial Institution Wire Name: the approved telegraphic abbreviation of the receiving financial institution's name; and
    - Special Handling Instructions: the specific delivery instructions for the receiving financial institution

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

The TreasuryDirect system exchanges information with the Federal Reserve Automated Clearing House (ACH) processing system. Debit and credit transactions are processed to support transactions in Treasury securities.

Fedwire Securities Services are used to transfer treasury securities between TreasuryDirect and the National Book Entry system (NBES). This supports the redemption of Treasury securities on the open market.

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?

Limited account-holder's banking information is shared with his/her financial institution to electronically process financial transactions. Corrections to financial information are submitted to the system in response to processed transactions.

3) **Accuracy, Timeliness, and Reliability**

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

      Personally Identifiable Information (PII) is provided directly by the individual during the account creation process. To successfully create an account, the individual's data is authenticated through a commercial verification service.

   b. **How will data be checked for completeness?**

      TreasuryDirect will audit each field to see that the data has the correct type and number of characters and that the data is in the correct format.

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

      Account holders have access to their TreasuryDirect account at any time via a secured Internet connection. They are encouraged to keep the information in the account current. TreasuryDirect customers can also contact customer service for updates and changes to the account. 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?**

      System data elements are described in the edit and error documentation of the system. Each field is described with the edits to be performed and error messages to be displayed along with the associated system processing.

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?**

   The data being collected will be used to verify the identity of the account holder and aid in the processing of transactions in Treasury securities.

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?**

The data collected will be used to build an account profile for the account holder. This profile will be used to process transactions in Treasury securities. Data is digitally maintained and filed.

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

The new data will all be incorporated in the account structure. The account holder will be able to access this information at any time via a secured Internet connection.

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

No.

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

System edits are applied to ensure 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. Account holders also have access to their account at any time via a secured Internet connection. They are encouraged to keep the information in the account current.

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 in any system other than in the TreasuryDirect system. Fiscal Service has sophisticated firewall security via hardware and software configurations as well as specific monitoring tools. Records are maintained in controlled access areas. Identification cards are verified to ensure that only authorized personnel are present. Electronic records are protected by restricted access procedures, including the use of passwords, sign-on protocols, multifactor authentication, and user authentication that are periodically changed. Only employees whose official duties require access are allowed to view, administer, and control the system records.

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. Client authentication provides protection between the client and the application that resides on the Fiscal Service computing infrastructure. This infrastructure has multiple layers of perimeter security including firewalls 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.

TreasuryDirect has an extensive inventory of automated system edits and input controls to prevent users from initiating erroneous and/or unauthorized transactions. New edits introduced to the system and existing edits are thoroughly tested prior to deployment.

To protect access to customer data, the customer is required to answer one of his/her security questions prior to editing data. Fields containing sensitive data (i.e. social security number, driver's license number, bank account number) are masked to prevent unauthorized viewing of the information. Only when the information is being edited is the entire field displayed. Also, new system functionality has been introduced that will lock an account down and prevent transactions from being processed if unauthorized activity is suspected.

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.)**

System data can be retrieved using an individual's account number or Taxpayer Identification Number. TreasuryDirect will permit searching with the account-holder's social security number to retrieve an account number. Searching can also be done on any valid unique information.

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 summary accounting and audit verification of transactions processed in the system. Account history and security history are maintained within the system. Queries can be run against the system database to track transactions for an account. The account profile is viewable but is only accessed to resolve problems and aid the account holder in processing transactions. Fiscal Service employees are given access to the system on a need to know basis.

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?**

Opening an account for the purposes of holding Treasury securities is a voluntary activity. As part of the account creation process, customers are provided and are required to agree to the terms and conditions of use. Privacy and legal notices are provided to the customer when they are opening a TreasuryDirect account. By agreeing to or completing and signing the forms, customers are granting consent to their information.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

Data within TreasuryDirect must be retained 5 years after all financial obligations have

been discharged and no security or account transactions that generate a history record have been transacted. Records can be deleted when the agency determines the records are no longer needed for administrative, legal, audit, or other operational purposes.

System documentation can be destroyed when superseded or obsolete, or upon the authorized deletion of the related master file or database, or upon the destruction of the output of the system if the output is needed to protect legal rights, whichever is latest.

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

System records will not be destroyed until management approval is obtained. System reports in paper form ready for disposal are destroyed by shredding or maceration. Definitive system records are stored in electronic media. These records are electronically erased using accepted techniques. Time frames for the destruction of records are documented in the system destruction schedule. This schedule is developed in accordance with guidelines from the National Archives and Records Administration (NARA).

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 Bureau of the Fiscal Service facility. The system is accessed from many personal computers in the homes and offices of account holders. A backup copy of system information is maintained at a secure offsite location.

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

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

Yes. Each system will create a system account profile. This profile will be used to process transactions in Treasury securities. The system will monitor the transactions to see that they are properly processed. In order to create the account the account holders must identify themselves by providing data that is verifiable.

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 account holder's 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):

Bureau of the Fiscal Service employees:
Access to system information is selectively granted based on the employee's need to perform his/her official duties. When an employee's duties change, then his/her access rights are changed accordingly or withdrawn entirely.

Employees are granted information access to perform the following duties:

- Process financial transactions for customers
- Respond to official inquiries regarding investment holdings
- Account for, reconcile and report financial transactions
- Audit and review the business and system processes
- Perform required reporting functions (such as interest income reporting to IRS)
- Oversee the management of the TreasuryDirect program
- Administer and manage the system
- Maintain the integrity of the system and its data

These records may also be disclosed to:
(1) Appropriate Federal, State, local, or foreign agencies or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order or license where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(2) 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 response to a court-ordered subpoena, or in connection with criminal law proceedings where relevant or potentially relevant to a proceeding;

(3) A Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) Agents or contractors who have been engaged to assist the Bureau of the Fiscal Service in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity;

(5) The Department of Justice when seeking legal advice or when
(a) The Department of the Treasury (agency), or

(b) The Bureau of the Fiscal Service, or

(c) Any employee of the agency in his or her official capacity, or

(d) Any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or

(e) The United States, where the agency determines that litigation is likely to affect the agency or the Bureau of the Fiscal Service, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation.

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.**

Logical access controls are the system-based mechanisms used to specify which individuals and/or processes are to have access to a specific system resource, and the type of access that is to be permitted. These controls limit users' access to information and restrict their access on the system to their designated level. Account holders will only have access to their own data. Access to system information is selectively granted based on the employee's need to perform his/her official duties. When an employee's duties change, then his/her access rights are changed accordingly or withdrawn entirely. There are

multiple unique role assignments that govern the user's access to the system and his/her capabilities. The system identifies the user's role based on the Logon ID and password provided.

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?**

No contractors are 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.

Savings Bond Replacement System (SaBRe)
SaBRe is a Fiscal Service application used to record and report transactions involving definitive holdings of U.S. Savings securities. TreasuryDirect and SaBRe exchange data to verify the accuracy of definitive U.S. Savings Bonds submitted for conversion to electronic form. The data exchanged is limited to description information of the bond (series type, denomination, serial number and security status), and does not involve personally identifiable or sensitive financial information of individuals. Information provided to SaBRe is viewed and used only by Fiscal Service employees.

Treasury Automated Auction Processing System (TAAPS)
TreasuryDirect receives U.S. Treasury marketable loan information from TAAPS through database connection(s). TreasuryDirect uses this information to process the required transactions (process interest payment amounts, calculate purchase price, etc.). The database connection(s) are used as a common repository for loan information (such as CUSIP, loan title, issuance date, auction results, interest payment dates, interest rates, etc.). This information is considered public information and is available at www.treasurydirect.gov. Internal personnel can query the database using the Global Securities Services (GSS) application.

Summary Debt Accounting System (SDAS)/Debt Information Management System (DIMS)
The systems interconnects with SDAS/DIMS to report a summary of all financial transactions (security issuances, security redemptions, etc.), and post daily and month-end balances.

Secure Payment System (SPS)
The SPS application provides a mechanism by which government agencies can create and certify payment schedules in a secure fashion.

Fiscal Service contracts with a private commercial firm to perform on-line verification of account holders establishing new primary accounts. This Verification Service (VS) provider uses specialized queries to access and compare verification data obtained from multiple independent data sources to assess the accuracy of the information provided by the account holder.

Accounting and Payments Application (APA)
TreasuryDirect and other TSS systems use APA to convert payment files into Treasury Disbursement Office (TDO) and Payment Automation Manager (PAM) acceptable formats.

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): Financial Institutions

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

Referring to the systems listed in the previous question, the following are the uses for the TreasuryDirect information.

Financial Institutions will use the data provided to them by TreasuryDirect to process financial transactions by debiting and crediting the account holder's designated account at a financial institution via the Automated Clearing House (ACH) network.

FedWire Securities Services will use the data provided to them by TreasuryDirect to process the transfer of securities between TreasuryDirect and the National Book-Entry System (NBES) that is maintained by the Federal Reserve System.

Internal Revenue Service will use the data Fiscal Service provides to record income and earnings information on account-holders as required by the Internal Revenue Code.

Social Security Administration will use the information provided to verify the holdings of Supplemental Security Income (SSI) and Medicare/Medicaid applicants and recipients and make decisions regarding their eligibility for benefits.

Courts and Law Enforcement Entities will use the information provided as required by law in the performance of their official duties. FRB will use the information to provide Customer Service support to customers.

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.