TreasuryDirect
Privacy Impact Assessment (PIA)

September 1, 2007

System Information

Name of System, Project or Program: TreasuryDirect
OMB Unique Identifier: 015350114011002004021 28

Contact Information

1. **Who is the person completing this document? (Name, title, organization, phone, email, address).**

   Pat Ahlborn, Director
   Division of Records Systems
   (304) 480-6272
   Pat.Ahlborn@bpd.treas.gov
   200 Third St Room 502
   Parkersburg, WV 26106-1328

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 St Room 501
   Parkersburg, WV 26106-1328

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

   Pat Ahlborn, Director
   Division of Records Systems
   (304) 480-6272
   Pat.Ahlborn@bpd.treas.gov
   200 Third St Room 502
   Parkersburg, WV 26106-1328

4. **Who is the Information Systems Security Manager who reviewed this document? (ISSM Name, title, organization, phone, email, address).**

   Jim McLaughlin, Information Systems Security Manager
   Division of Program Services
   (304) 480-7972
   Jim.Mclaughlin@bpd.treas.gov

200 3rd Street Room 409
Parkersburg, WV 26106-1328

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

   Denise Hofmann, Disclosure Officer
   Division of Administrative Services, Information Management Branch
   (304) 480-8402
   Denise.Hofmann@bpd.treas.gov
   200 Third St Avery A4-A
   Parkersburg, WV 26106-1328

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

   Kim McCoy, Assistant Commissioner
   Office of Information Technology
   (304) 480-6635
   Kim. McCoy@bpd.treas.gov
   200 Third St
   Parkersburg, WV 26106-1328

System Application/General Information

1. **Does this system contain any information in identifiable form?**

   Yes. The TreasuryDirect system contains a number of personally identifiable fields. For a complete list see the answer to question 2e under data in the system.

2. **What is the purpose of the system/application?**

   The purpose of the TreasuryDirect system is to support Public Debt business processes, process electronic services to the public (E –government), and improve services to investors in Treasury securities.

3. **What legal authority authorizes the purchase or development of this system/application?**

   The legal authority for operating the TreasuryDirect system is contained in:

   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.)**

   Public Debt issued a System of Records notification for TreasuryDirect. The notice was published in the Federal Register dated May 22, 2001, under the title of BPD.008-Retail Treasury Securities Access Application (the system's original name at its early developmental stage).

   Public Debt had previously published two other notices that define the terms and conditions governing the routine use of customer information (5 U.S.C. Section 552a (b) (3)), which is in addition to BPD.008 that specifically addresses records maintained on the system. These notices are: BPD.002 for United States Savings-Type Securities, and BPD.003 for United States Securities (Other than Savings-Type Securities).

Data in the System

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

   Records in the TreasuryDirect system cover those individuals who own or make inquiries concerning United States Treasury securities.

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

   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?**
   In most cases the information is provided by the individual covered by this system or, with their authorization, is derived from other systems of records.

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

   The TreasuryDirect system exchanges information with the Federal Reserve 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.

   c. **What State and/or local agencies are providing data for use in the system?**

   No State and/or local agencies are providing data for use in the system.

d. 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.

e. What information will be collected from the employee and the public?

The only information collected from a Bureau employee is his/her logon-id and password. This information is checked against the Bureau login system and if they match the employee is allowed access to the system.

The following information is requested from the TreasuryDirect accountholder and is received by the system via a secured Internet connection.

Account-holder's Name, which includes:
- first name (required);
- middle name or initial (optional);
- last name (required); and
  suffix (optional).

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.

Account-holder's Social Security Number (SSN) (required)

The SSN 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 (post office box not is acceptable);
- City;
- State; and
- Zip Code.

Account-holder's driver's license or state identity card information (optional), which includes:

- License/Identification number
- Issuing state
- Expiration date

Account-holder's alternate telephone numbers, such as Work and Cell (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)

TreasuryDirect account password: a string of alphanumeric and special characters (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), which 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.

Throughout the account establishment process, a potential account-holder has the option to cancel the transaction. If he/she elects to cancel the transaction, then information provided up to that point is not retained by the system.

Of course, the purchase of a U.S. Treasury security is purely voluntary. The information we request, as cited above, is the minimum necessary to service the account-holder and verify his/her identity.

3. Accuracy, Timelines, and Reliability

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

TreasuryDirect uses the on-line verification service Pay.gov to verify the accuracy of data provided by a potential account-holder when he/she is establishing a primary account. If the information provided is not verified, account access is blocked until a form certifying the account data is provided. Usually, financial information is processed through the ACH system to ensure that it is correct prior to financial transactions being processed in the account.

b. How will data be checked for completeness

The TreasuryDirect system will edit 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. 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.)

Account holders have access to their account at any time via a secured Internet connection. They are encouraged to keep the information in the account current. Processing errors in the system involving incorrect information are handled quickly.

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

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. **Is the use of the data both relevant and necessary to the purpose for which the system is being designated?**

   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, and 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. The account will contain information about the treasury security holdings of the accountholder (issues, redemptions, payments, financial information etc.).

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/public that would not be possible without the new data?**

   The system needs the requested data to verify the identity of the customer and to determine the accountholder's suitability to process transactions in Treasury securities.

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

   TreasuryDirect uses the on-line verification service Pay.gov to verify the identity of a potential account-holder when he/she is establishing a primary account. If the information provided is not verified, account access is blocked until a form certifying the account data is provided. System edits are used to ensure the data is in the correct format. New and corrected financial data is passed through the ACH system prior to transactions being processed. Account holders 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?**

Public Debt 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, 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. A 128-byte encrypted Secured Socket Layer (SSL) client authentication provides protection between the client and the application that resides on Public Debt's 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.

Requiring the customer to answer one of his/her security questions prior to editing data protects access to sensitive information. 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. Public Debt's computing infrastructure is subject to frequent independent audits and regular security reviews.

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.

The system data can be retrieved using the 10-digit account number. Searching with the account-holder's social security number can retrieve account numbers. Searching can also be done on any valid unique information.

9. **What kinds 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. There is no capability to track transactions entered on a specific account. The account profile is viewable but is only accessed to resolve problems and aid the account holder in processing transactions. Public Debt employees are given access to the system on a need to know basis.

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?**

   The system is maintained at a Bureau of the Public Debt facility. The system is accessed from many personal computers in the homes and offices of accountholders. A backup copy of system information is maintained at a secure offsite location.

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

   TreasuryDirect system records 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 de 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.

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?**

   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).

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

TreasuryDirect has recently introduced the use of access cards for account holders to gain access to the system. Access cards are used as a form of second factor authentication.

5. How does the use of this technology affect public/employee privacy?

The use of access cards affects the security of the system. The use of the card strengthens the security of the logon process by introducing second factor authentication into the system.

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

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

7. What kinds of information are collected as a function of the monitoring of individuals?

Records of holdings in treasury securities, financial information, and system access logs record system transactions used by the accountholder in processing transactions.

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 of Public Debt who are subject to personnel screening procedures and to the Treasury Department Code of Conduct or by agents of Public Debt who are required to maintain proper control over records while in their custody. 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. For those categories of records stored in computers with online terminal access, the information cannot be accessed without proper passwords and preauthorized functional capability.

9. **Under which Privacy Act SORN does the system operate? Provide number and name.**

   Public Debt issued a System of Records notification for TreasuryDirect. The notice was published in the Federal Register dated May 22, 2001, under the title of BPD.008-Retail Treasury Securities Access Application (the system's original name at its early developmental stage).

   Public Debt had previously published two other notices that define the terms and conditions governing the routine use of customer information (5 U.S.C. Section 552a (b) (3)), which is in addition to BPD.008 that specifically addresses records maintained on the system. These notices are: BPD.002 for United States Savings-Type Securities, and BPD.003 for United States Securities (Other than Savings-Type Securities).

10. **If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.**

    The existing Privacy Act system of records, which covers TreasuryDirect, was not substantially revised in FY 2006. http://ntpdweb.bpd.treas.gov/er/systems.pdf

Access to Data

1. **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others.)**

   The primary users of data in the system will be:

   Account holders:
   Account holders have access to their account at any time via a secured Internet connection.

   Bureau of the Public Debt 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 Public Debt 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 Public Debt, 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 Public Debt, 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?

To gain access to the system, the employee's supervisor must submit a written access request to the TreasuryDirect Data Owner and Information System Security Officer (ISSO) , or their designated representative, for their review and approval. The supervisor is thereafter responsible for periodically reviewing and certifying that the access rights of his/her employees are necessary to perform

official duties. This review is conducted at least once every two years. In addition to role assignments, the system has an extensive inventory of automated system edits and controls to further regulate user access.

BPD 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. 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? (list processes and training materials.)**

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.
Public Debt employees receive training classes and instructional materials to further improve their handling of sensitive information and understanding of security issues. All TreasuryDirect users receive regularly scheduled security awareness refresher training, which is required by Public Debt policy. System users are trained in the security controls of the system, including rules of behavior and the consequences of violating the rules. We also provide our employees with regularly updated instructional material (both printed and posted on our Intranet website) on security issues

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, were Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

No contractors are currently involved with the design, development and maintenance of the system.

6. Do other systems share data or have access to the data in the system? If yes, explain.

Five systems have a direct interface or share data with the TreasuryDirect system. They are:

Pay.gov

TreasuryDirect uses the on-line verification service Pay.gov to verify the identity of a potential account-holder when he/she is establishing a primary account. Pay.gov is a Treasury-approved verification engine maintained by the Financial Management Service (FMS).

Pay.gov uses multiple third-party databases (such as Equifax, TeleCheck, RAF, etc.) to perform on-line and real-time identity verification by querying both local and remote data sources via secured connections. After performing this query, Pay.gov assigns a confidence score to the reliability of the information provided, which is then transmitted to TreasuryDirect. TreasuryDirect interprets this confidence score, and the appropriate response is presented to the potential account-holder. Information exchanges between TreasuryDirect and Pay.gov are transmitted over a secured link.

A potential account-holder must submit the following information for identity verification. Pay.gov does not retain this information after it completes the verification process.

- Name
- Social Security number
- Date of birth
- Address
- Home phone
- Work phone
- Cell phone
- E-mail address
- Driver's license/state identification information (number, issuing state, and expiration date)

Savings Bond Replacement System (SaBRe)

SaBRe is a Public Debt 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 Public Debt employees.

Global Securities System (GSS) Interface

TreasuryDirect interfaces with GSS to obtain data on U.S. Treasury marketable loans. The system then uses this information to process the required transactions (process interest payment amounts, calculate purchase price, etc.). GSS is used as a common repository for loan information (such as CUSIP, loan title, issuance date, auction results, interest payment dates, interest rates, etc.).

Public Debt Accounting and Reporting System (PARS) Interface

The TreasuryDirect system also interconnects with PARS to report a summary of all financial transactions (security issuances, security redemptions, etc.), and post daily and month-end balances.

Identity Guard (IDG)

TreasuryDirect interfaces with Identity Guard to provide two-factor authentication to the system via access cards. The systems keep track of the customer account number and access card number. The customer must enter the grid information from the access cards to log in to TreasuryDirect. Information in IDG is viewed and used only by Public Debt employees.

7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

All BPD employees who have access to information in a Privacy Act system have some responsibility for protecting personal information covered by the Privacy Act. The information owner, system manager, and ultimately the BPD CIO have the responsibility to see that the data is protected from all threats.

8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?

Several agencies share data and information with the TreasuryDirect system. They are:

Pay.gov

TreasuryDirect uses the on-line verification service Pay.gov to verify the identity of a potential account-holder when he/she is establishing a primary account.

Pay.gov is a Treasury-approved verification engine maintained by the Financial Management Service (FMS).

Pay.gov uses multiple third-party databases (such as Equifax, TeleCheck, RAF, etc.) to perform on-line and real-time identity verification by querying both local and remote data sources via secured connections. After performing this query, Pay.gov assigns a confidence score to the reliability of the information provided, which is then transmitted to TreasuryDirect. TreasuryDirect interprets this confidence score, and the appropriate response is presented to the potential account-holder. Information exchanges between TreasuryDirect and Pay.gov are transmitted over a secured and encrypted Virtual Private Network (VPN) link.

A potential account-holder must submit the following information for identity verification. Pay.gov does not retain this information after it completes the verification process.

- Name
- Social Security number
- Date of birth
- Address
- Home phone
- Work phone
- Cell phone
- E-mail address
- Driver's license/state identification information (number, issuing state, and expiration date)

Financial Institution Information

Limited account-holder's banking information is shared with his/her financial institution to electronically process financial transactions. A TreasuryDirect account-holder must have an active account at a U.S. based financial institution. All purchase and payment transactions processed through TreasuryDirect are made by directly debiting or crediting the account-holder's designated account at a financial institution via the Automated Clearing House (ACH) network. Financial institutions provide the initial defense against fraudulent or unauthorized transactions. Public Debt verifies the account-holder's bank account information (ABA routing number, account number and account type) every time the account-holder adds new banking information or edits existing information. The information shared is limited to the following:

- the account-holder's TreasuryDirect account number;
- the dollar amount of the transaction;
- the type of financial transaction (debit or credit); and

- the account-holder's banking information (name of the financial institution, account number, ABA routing number; names on the account; and account type - checking or savings).

FedWire Securities Services

Upon the account-holder's request, we will wire-transfer eligible book-entry securities under his/her control to another book-entry system maintained by a financial institution or brokerage firm. We execute this transfer using the Federal Reserve's FedWire Securities Services. The FedWire Securities Service is a secured communications network linked to the National Book-Entry System (NBES) that is maintained by the Federal Reserve System. The information provided by the account-holder, via a secured Internet connection, is transmitted to the book-entry system receiving the security. The information shared is limited to the following:

- 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.

Other Government Agencies

Public Debt provides income earnings information on account-holders to the Internal Revenue Service (IRS) to comply with the Internal Revenue Code.

Public Debt provides to the Social Security Administration (SSA) information regarding the investment holdings of certain TreasuryDirect account-holders. This information is provided to comply with the terms of computer matching agreements between Public Debt and SSA, which are published in the Federal Register. SSA is the initiator of these agreements. SSA uses the information provided to verify the holdings of Supplemental Security Income (SSI) and Medicare/Medicaid applicants and recipients. SSA provides Public Debt with the names and Social Security Number of individuals whose investment holdings it wishes to verify. Public Debt cross-matches this list against the system's database, and provides SSA with the total par amount of Series E, EE and I U.S. Savings Bonds for the account-holders identified.

Courts and Law Enforcement Entities

In accordance with Title 5 U.S.C. Section 552a (b), Public Debt is permitted to release customer information in response to a subpoena or order issued by a U.S.-based court. We are further permitted to release information to other government

organizations to enable them to perform their official duties. These other government organizations are:

- law enforcement agencies on the federal, state or local level;
- employees or representatives of the General Accounting Office (GAO); and
- members of Congress, or their authorized representatives.

A government organization requesting access to customer information must:

- submit the request in writing to Public Debt;
- identify the specific information needed; and
- specify the official nature of the request (such as a criminal investigation, audit, etc.).

A Public Debt official determines whether the organization's need for the information is justified, and responds to the request based on that determination.

9. How will the data be used by the other agency?

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

Pay.gov will use the data to perform on-line and real-time identity verification by querying both local and remote data sources via secured connections. After performing this query, Pay.gov assigns a confidence score to the reliability of the information provided, which is then transmitted to TreasuryDirect. TreasuryDirect interprets this confidence score, and the appropriate response is presented to the potential account-holder. Information exchanges between TreasuryDirect and Pay.gov are transmitted over a secured and encrypted Virtual Private Network (VPN) link. Pay.gov does not retain this information after it completes the verification process.

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 Public Debt 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.

10. Who is responsible for assuring proper use of the data?

All BPD employees who have access to the system, the system owner, system manager, and the BPD CIO share responsibility for assuring the proper use of data in the system.

The Public Debt Disclosure Officer is responsible for administering requests for system data submitted to the Bureau involving the Privacy Act. Public Debt fully complies with the provisions of the Freedom of Information Act (FOIA), Title 5 U.S.C. Section 552, and the Privacy Act, Title 5 U.S.C. Section 552a. Public Debt provides an established procedure to solicit requests to review and correct information recorded, and we have a dedicated Disclosure Officer who manages and administers the program.