TreasuryDirect Privacy Impact Assessment (PIA)

September 1, 2006

Agency:	**U.S. Department of the Treasury**
Bureau:	**Bureau of the Public Debt**
Account Identification Code:	**015-35-05-6000-0**
Unique Project (Investment) Identifier:	**015350114011002004021 28**

Introduction: System Description

The TreasuryDirect system is an Internet-based application that enables private citizens to open an account, buy eligible U.S. Treasury obligations, and manage their accounts and security holdings. The system provides account-holders with an easy and secure way of viewing and managing all of their Treasury security holdings online from one convenient location with minimal customer service assistance.

Sections I, II and III: Description of Information Collected, Why Information is Requested and the Intended Use of the Information

Public Debt designed the system specifically to operate with a minimal amount of the account-holder's personally identifiable information. The primary purpose of requesting this information is to conduct financial transactions in a purely electronic and Internet-based environment. The financial transactions processed include:

- collecting funds owed for the purchase of securities via Automated Clearinghouse (ACH):
- paying interest and redemption payments resulting from these investments via ACH;
- processing the wire transfer of eligible book-entry securities via the Federal Reserve's FedWire Securities Service.
- recording and reporting income earned by account-holders to the Internal Revenue Service (IRS); and
- recording and reporting investment transactions to account for the resulting public debt.

A secondary purpose for collecting this information is to thoroughly verify the account-holder's identity. We verify the customer's identity to:

- mitigate the risk of identity theft;
- protect the financial interest of the United States federal government; and
- meet the various anti-money laundering and anti-terrorist financing requirements mandated by the federal government.

Ia Description of Information Collected	Ib Source of the Information Collected	II Why the Information is Collected	III Intended Use of the Information
Account-holder's Name, which includes: • first name (required); • middle name or initial (optional); • last name (required); and • suffix (optional).	Provided by the account-holder via a secured Internet connection.	• Establish an account. • Verify the account-holder's identity. • Identify the account-holder. • Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.	• Establish an account. • Verify the account-holder's identity. • Identify the account-holder. • Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.
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; d) owner(s) of gift securities purchased or converted by the account-holder.	Provided by the account-holder via a secured Internet connection.	• Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.	• Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.

Ia Description of Information Collected	Ib Source of the Information Collected	II Why the Information is Collected	III Intended Use of the Information
Account-holder's Social Security Number (SSN) (required)	Provided by the account-holder via a secured Internet connection.	• Establish an account. • Identify the account-holder. • Verify the account-holder's identity. • Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.	• Establish an account. • Identify the account-holder. • Verify the account-holder's identity. • Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.
The SSN of other parties (see above definition) - (required).	Provided by the account-holder via a secured Internet connection.	• Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.	• Register legal ownership of U.S. Treasury obligations. • Manage the account-holder's account and investment holdings. • Perform required IRS reporting functions.
Account-holder's email address (required)	Provided by the account-holder via a secured Internet connection.	Email is the primary mode of communicating with the account-holder.	• Contact the account-holder to communicate information regarding his/her account and investments. • Notify the account-holder of changes in his/her account and investment holdings.
Account-holder's home telephone number (required)	Provided by the account-holder via a secured Internet connection.	• Contact the account-holder to communicate information regarding his/her account and investments. • Verify the account-holder's identity.	• Contact the account-holder to communicate information regarding his/her account and investments. • Verify the account-holder's identity.

Ia Description of Information Collected	Ib Source of the Information Collected	II Why the Information is Collected	III Intended Use of the Information
Account-holder's home address (required), which includes: • Full street address (post office box not is acceptable); • City; • State; and • Zip Code.	Provided by the account-holder via a secured Internet connection.	• Verify the account-holder's identity. • Contact the account-holder to communicate information regarding his/her account and investments. • Perform required IRS reporting functions.	• Verify the account-holder's identity. • Contact the account-holder to communicate information regarding his/her account and investments. • Perform required IRS reporting functions.
Account-holder's drivers license or state identity card information (optional), which includes: • License/Identification number • Issuing state • Expiration date	Provided by the account-holder via a secured Internet connection.	Verify the account-holder's identity.	Verify the account-holder's identity.
Account-holder's alternate telephone numbers, such as Work and Cell (optional)	Provided by the account-holder via a secured Internet connection.	Provide an alternate means to contact the account-holder.	Provide an alternate means to contact the account-holder.
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).	Provided by the account-holder via a secured Internet connection.	• Transact financial business with the account-holder. • Verify the account-holder's identity.	• Transact financial business with the account-holder. • Verify the account-holder's identity.
TreasuryDirect Account Number (required)	Initially generated by the system upon establishment of the account, and thereafter provided by the account-holder via a secured Internet connection.	• Identify an account • Authenticate the account-holder	• Identify an account • Authenticate the account-holder

Ia Description of Information Collected	Ib Source of the Information Collected	II Why the Information is Collected	III Intended Use of the Information
TreasuryDirect account password, a string of alphanumeric and special characters (required).	Provided by the account-holder via a secured Internet connection.	Authenticate the account-holder	Authenticate the account-holder
Password Hint, a line of text to remind the account-holder of his/her password (required).	Provided by the account-holder via a secured Internet connection.	Assist the account-holder.	Account-holder uses the function to remind him/her of a forgotten password.
Authentication Questions and Answers, responses to three of ten standardized questions (required).	Provided by the account-holder via a secured Internet connection.	Authenticate the account-holder	Authenticate the account-holder
Account-holder's date of birth (required).	Provided by the account-holder via a secured Internet connection.	Verify both the account-holder's identity and his/her status as a legal adult.	Verify both the account-holder's identity and his/her status as a legal adult.
Minor child's date of birth (required if establishing a minor account).	Provided by the account-holder via a secured Internet connection.	• Verify the child's legal status as a minor. • Determine when the minor child becomes a legal adult (defined as 18 years of age).	• Verify the child's legal status as a minor. • Determine when the minor child becomes a legal adult (defined as 18 years of age).
Security registration (required), which includes type of registration and owner(s)' full name(s).	Provided by the account-holder via a secured Internet connection.	• Record legal ownership of the security. • Manage the account-holder's investment holdings. • Perform required IRS reporting functions.	• Record legal ownership of the security. • Manage the account-holder's investment holdings. • Perform required IRS reporting functions.

Ia Description of Information Collected	Ib Source of the Information Collected	II Why the Information is Collected	III Intended Use of the Information
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.	Provided by the account-holder via a secured Internet connection.	To transmit eligible book-entry securities via the FedWire Security Service.	To transmit eligible book-entry securities via the FedWire Security Service.

Section IV: With Whom System Information is Shared

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)

FMS successfully completed a Certification and Accreditation (C&A) review of Pay.gov in June 2005. As a result of this review, the system was granted full Authorization to Operate (AO), which is valid through March 2008.

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.

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.

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.

Bureau of the Public Debt Employees

In accordance with Title 5 U.S.C. Section 552a (b) (1) and (2), Public Debt controls employee access to account-holder information. 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

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.

To further ensure that employees limit their access to customer information to legitimate and authorized business uses, the system uses logical access controls to regulate user behavior. 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. 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.

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) 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.

TreasuryDirect also has additional controls to protect the integrity of the application and the confidence of the public in the application. The system uses functionality that detects and stops suspected attempts to manipulate or insert unauthorized data and programming code changes into the system. The system infrastructure has also been configured to restrict access to sensitive customer service functionality. Technical personnel also monitor Internet activity to detect unauthorized activity.

Section V: Opportunities to Decline/Consent to Uses of Information

Public Debt provides convenient hyper-links to information regarding Privacy, Security, Legal/Regulatory issues and the terms and conditions governing the system. These hyper-links are located throughout the system and throughout Public Debt's overall public website. Public Debt also maintains on TreasuryDirect an interactive guided tour of the system that users can readily access online. This tour addresses what information is needed to establish an account, and how Public Debt will use this information. Public Debt also responds to "Frequently Asked Questions" via hyper-links in the system that address the use of personally identifiable information collected from the customer.

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.

An account-holder can access his/her account and review the information recorded at any time via an Internet connection. A TreasuryDirect account-holder can allow edit the following items of information on-line:

- Address;
- Home, work, and cell phone numbers;
- Email address;
- Driver License/State Identification information (including number, issuing state, and expiration date);
- Bank information (including routing number, account number, name(s) on account, and type of account);
- Security registration information; and
- Personalized account name.

Account-holders wishing to change other informational items (such as name or Social Security Number) can do so by contacting our customer service staff. Only our customer service staff can change such information if the account-holder submits suitable legal evidence that justifies such a change.

An account-holder has several avenues to contact Public Debt:

- A "Contact Us" feature available in all accounts. This feature enables the account-holder to send inquiries directly to the customer service staff via a secured within-system connection. This feature, though, cannot be used for secured two-way communication. The customer service staff can only reply to such inquiries via standard email (which is not secured), telephone or physical mail

- A general Public Debt email address for unsecured communications.

- A dedicated direct telephone number to contact customer service personnel. This telephone number, until January 2007, is (304) 480-USTD (x8783). After that date, (304) 480-7711.

- A specifically designated Post Office box maintained by the Office of Investor Services for delivery of physical mail.

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. Information on Public Debt's FOIA/Privacy Act program is provided through the following channels:

- A direct FOIA/Privacy Act request email link through Public Debt's public website.
- Detailed public notices posted on this public website with hyper-links at relevant locations throughout the site. A direct link to these notices is also provided within the system.
- Informational brochures and circulars produced by Public Debt and available at participating financial institutions.
- Official government publications addressing Public Debt programs (such as the Federal Register and the Code of Federal Regulations) published by the U.S. Government Printing Office.

Section VI: How Information is Secured

The information collected and maintained on TreasuryDirect is categorized as Sensitive But Unclassified (SBU). Public Debt has implemented suitable system, personnel and physical security measures to adequately protect the integrity and security of this information.

System Security Measures: TreasuryDirect meets the specific security requirements established by the Federal Information Security Management Act (FISMA), OMB Circular A-130 and guidance from the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). The system was first certified to be compliant with these provisions as a result of an OMB A-130 Certification and Accreditation (C&A) security review completed in September 2002. Public Debt completed the system's most recent C&A review in August 2006. On August 8, 2006, the Authorizing Official for the system certified that the system is compliant with the federal standards cited above and is authorized to continue operations. This accreditation is valid through August 2007.

In addition to periodic C&A security reviews, TreasuryDirect maintains the following controls to ensure that continuous monitoring of the system is performed:

- A NIST 800-26 Self-Assessment is completed each year on the system. The most recently completed self-assessment was completed on March 2, 2005. No subsequent assessment has been done as the system has undergone three successive Certification and Accreditation(C&A) processes. The C&A process is more rigorous than the self-assessment.
- The system's Configuration Management Plan is reviewed and updated at least once a year. This plan is usually reviewed and updated with the implementation of each system release. The system is currently upgraded with a release three times per year.
- The system's Security Plan is reviewed and updated at least once a year. System security controls and automated edits are reviewed and tested at least once per year.

- All maintenance and enhancement work performed on the system's programming and code is managed through Public Debt's Change Management process.

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 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.

Personnel Security Measures: Public Debt has implemented a detailed security infrastructure to ensure that all employees have been screened and can be afforded a level of trust commensurate with the duties of the individual. These measures comply with the Office of Personnel Management (OPM) human resource guidelines**.**

Background investigations (in accordance with Executive Orders 12958 and 12968; OMB Circular No. A-130; and Title 5 of the Code of Federal Regulations sections 731, 732, and 736) are conducted on all newly hired Public Debt employees. Regular background reinvestigations are conducted on existing employees as a condition of continued employment. These reinvestigations are conducted approximately every five years. Positions are reviewed to ensure they have been classified at the proper sensitivity level during these investigations and reinvestigations.

Physical Security Measures: Physical security at Public Debt buildings includes x-raying all hand carried items by person(s) entering the buildings. Armed security guards are posted throughout our facilities for 24-hour coverage, seven (7) days a week. The exterior of the buildings are monitored with a closed-circuit television and a videocassette recorder system.

Armed security guards monitor access to our buildings. Walk-through and hand-held metal detectors are used to scan for prohibited items. Entry to the buildings is only permitted to individuals with valid Public Debt-issued ID cards, which are validated by a card reader system. The card reader provides the security guard visual and audible signals validating authorized access. This measure prevents unauthorized persons from gaining entry by using a lost or stolen ID card. All interior doors are equipped with dual combination key and cipher locks, which have been guaranteed by the manufacturer to be unique in the area.

Contingency and Business Continuity Planning: The programming code and system data are backed up on a regular schedule (nightly, weekly, and monthly) and stored both on-site and off-site in secured, access-restricted locations. An image copy of system data is also continuously captured and transmitted to an off-site mainframe computer. This off-site computer resides in a geographic area that is well removed from the system's physical location.

Public Debt maintains two contingency sites to support the system. One site is located within the same geographic region. The second site is located in another geographic region out of state where a duplicate and independent TreasuryDirect system is maintained in a secured and access-restricted facility. In the event of a disaster or system failure, systems users can be switched over to either site, and continue operations. In addition to plans to ensure business continuity, we maintain automated processes and procedures to address short-term disruptions in the system's ancillary functions.

Section VII: System of Records Notification

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).

Section VIII: The Consequences of Collecting/Flow of Information

The system was designed specifically to enable investors in U.S. Treasury securities to process their own transactions with minimal to no customer service support via the Internet. A potential risk of this design is that critical SBU information involving personal finances could become vulnerable to interception by unauthorized parties. To effectively mitigate this risk, all information keyed by the account-holder and displayed to him/her is transmitted over a secure socket layer (SSL) connection using a minimum 128-bit encryption. Access to an account is controlled with an account number and password entered via a virtual keyboard to reduce the threat of key-logging or similar unauthorized surveillance attempts. The account-holder must provide both data elements to authenticate his/her identity and gain access to account information. TreasuryDirect also provides two tools to assist account-holders who have forgotten their passwords. Both of these tools require the user to authenticate him/herself by providing exact and specific responses to standardized questions that are only known to the account-holder.

Another potential risk is that Public Debt personnel could access customer information for unauthorized purposes. To mitigate this risk, procedural and systemic controls are in place to detect such misuse. These controls are fully described above in sections IV and VI.

A positive consequence of this approach is that the flow of customer information is being centralized to a single and controllable source – the system. Previously, transactions were processed in a semi-manual or purely manual environment. Under these conditions, sensitive information was received through multiple avenues (physical mail, telephonic, etc.), and was handled by multiple employees, thus increasing the number of individuals having access to such information. With the current system, little to no personnel routinely see such information because the account-holder is independently processing most of his/her transactions through the system.

Section IX: Alternatives to Collecting and Handling Information

As indicated above, the system was designed to fully enable customer self-sufficiency in a near real-time electronic environment. This design directive limited Public Debt to a real-time and interactive Internet-based application because the use of an off-line system would represent a "step-back" that runs counter to the President's Management Agenda.

The system's design team also considered and analyzed various alternatives to authenticating the account-holder's identity. The team researched various authentication methods to determine which alternative would best reduce threats and vulnerabilities and still be cost effective for Public Debt. Authentication methods analyzed included account number with password, third party verification services, digital certificates, and biometrics. Although the use of digital certificates and biometrics offer more stringent security, the cost was too high for the anticipated number of customers expected for the system. Also, the use of such devices was expected to significantly reduce the number of potential customers, since such technologies have not become commercially viable for the general public.

The team also evaluated third-party verification services such as eCheck Secure and Equifax, but found that the cost per transaction made it cost-prohibitive considering the number of transactions that TreasuryDirect will eventually process per year. After careful analysis, it was decided that the TreasuryDirect would use an account number with password combination and a third party verification service for account establishment. The third party verification service is Pay.gov, which is fully described above.

Section X: Risk Mitigation Measures

A thorough risk inventory analysis was conducted on the system during its design phase. This inventory is re-examined and re-assessed at least annually to address new developments, and the current version addresses 19 risks factors.

The salient points of this risk analysis that directly address PIA related issues are as follows.

Area of Risk	Surety (Asset Protection) Considerations
Description of the Risk	Catastrophic failure and/or loss of the system.
Mitigation Strategy	Have a disaster recovery plan in place that is regularly reviewed and updated. Establish a designated back-up facility. Implement a routine of backing up system data to facilitate a reliable system restore in the event of an emergency. Assign dedicated personnel for emergency support functions. Maintain (and regularly update) a contact sheet of emergency support personnel.
Current Status	The programming code and system data are backed up on a regular schedule (nightly, weekly, and monthly) and stored both on-site and off-site in secured, access-restricted locations. An image copy of system data is also continuously captured and transmitted to an off-site mainframe computer. This off-site computer resides in a geographic area that is well removed from the system's physical location. Public Debt maintains two contingency sites to support the system. One site is located within the same geographic region. The second site is located in another geographic region out of state where a duplicate and independent TreasuryDirect system maintained in a secured and access-restricted facility. In the event of a disaster or system failure, systems users can be switched over to either site, and continue operations. In addition to plans to ensure business continuity, we maintain automated processes and procedures to address short-term disruptions in the system's ancillary functions. Significant back-up functionality has been built to lower the possibility of a catastrophic failure of the system.

Area of Risk	Security
Description of the Risk	System and its supporting infrastructure fail to keep pace with security requirements, affecting the reliability of the information or the system. The level of risk associated with this potentiality is high.
Mitigation Strategy	Maintain a system-specific security plan that is reviewed by IT security specialists with each subsequent release and updated accordingly. Incorporate security testing into each release's development/deployment test. Address problem areas identified during review and/or test. Ensure that personnel who work with or on the system are properly trained in IT security measures. Ensure that both the system is secured and that only reliable and trust-worthy personnel are permitted to work with or on the system.
Current Status	TreasuryDirect meets the specific security requirements established by the Federal Information Security Management Act (FISMA), OMB Circular A-130 and guidance from the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). The system was first certified to be compliant with these provisions as a result of an OMB A-130 Certification and Accreditation (C&A) security review completed in September 2002. Public Debt completed the system's most recent C&A review in August 2006. On August 8, 2006, the Authorizing Official for the system certified that the system is compliant with the federal standards cited above and is authorized to continue operations. This accreditation is valid through August 2007. In addition to periodic C&A security reviews, TreasuryDirect maintains the following controls to ensure that continuous monitoring of the system is performed. A NIST 800-26 Self-Assessment is completed each year on the system, when required. The system's Configuration Management Plan is reviewed and updated at least once a year. This plan is usually reviewed and updated with the implementation of each release, which makes the usual cycle for review (currently, three times per year). The system's Security Plan is reviewed and updated at least once a year. This plan is usually reviewed and updated with the implementation of each release, which makes the usual cycle for review (currently, three times per year). System security controls and automated edits are reviewed and tested with the implementation of each release. After the planned cycle of system releases are completed, these controls will be reviewed and tested at least once per year. All maintenance and enhancement work performed on the system's programming and code is managed through Public Debt's Change Management process.

Area of Risk	Privacy
Description of the Risk	System fails to adequately protect customer information
Mitigation Strategy	Limit the volume of investors' personally identifiable information collected. Maintain systemic controls to protect system accessibility. Maintain an effective and thorough IT security program for the system.
Current Status	Privacy issues are paramount in the system's development and continued maintenance of the system. Public Debt only collects information from account-holders that is necessary to verify their identities, authenticate identities upon access and transact business. Passwords are required to obtain access to this information and accounts are locked after three consecutive unsuccessful attempts. To further ensure that system access is controlled, the system has a 128-bit encryption to ensure the data when being transmitted via the internet. Automated security controls are routinely tested by Public Debt personnel. Access to account information and the level of this access is restricted. Public Debt employees are only granted enough system ability that is sufficient to perform his/her official job responsibilities – and no more. Procedural, systemic and management controls are in place to ensure that these restrictions are enforced.

Section XI: Rationale for the Final System Design

The executive management of Public Debt established the following design principals to govern the system's development and continued operations:

- Provide a single Internet portal for Public Debt's retail products and online services;
- Establish a stronger identity and common positioning for Public Debt's products in the financial marketplace and the world of electronic commerce;
- Reinforce Public Debt's retail relationship with account-holders; and,
- Promote account-holder self-sufficiency using interactive technologies.

The overall purpose of these principals was to provide Public Debt with a means of further achieving its strategic goals of:

- Minimizing the cost of the Federal government's borrowing; and
- Providing mechanism for participation by a wide range of investors in Treasury debt financing..

Section XII: Informational Life Cycle Analysis

Public Debt has implemented a records management procedure to ensure the correct and proper retention and ultimate disposal of systemic and business records for the system. This procedure was established based on regulatory guidance provided by the National Archive and Records Administration (NARA). This guidance addresses the general records requirements as cited in the relevant sections of General Records Schedule (GRS) 20 and 24, and the specific guidance set forth for electronic records as cited in NARA Bulletin 2003-02.

PD F 5055 E
Department of the Treasury
Bureau of the Public Debt

RECORD OF COORDINATION AND APPROVAL

IDENTIFICATION NO.

TYPE DOCUMENT
☐ Treasury Directive Manual Chapter ☐ Treasury Directive Amendment ☐ Treasury Bulletin ☐ Treasury Order ☑ Other (Specify) TreasuryDirect System Privacy Impact Assessment

SUBJECT	PERSON TO CONTACT		
	NAME	OFFICE	TELEPHONE NO.
Privacy Impact Assessment (PIA)	Denise Hofmann	OMS	304/480-8402

EXPLANATION

This is the final draft of TreasuryDirect's Privacy Impact Assessment (PIA) to incorporate security changes made to the system in the Galileo release.

RELEASED FOR COORDINATION

TITLE	SIGNATURE	DATE	DEADLINE DATE FOR COORDINATION
Disclosure Officer	Denise K. Hofmann	09/15/06	09/29/06

ADDRESSEES WILL BE RECORDED AS CONCURRING IF NO RESPONSE IS RECEIVED BY THE DEADLINE DATE FOR COORDINATION

OFFICE/OFFICIAL	SIGNATURE	DATE	CONCUR		NON-CONCUR	COMMENT ADOPTED
			No Comment	Comment		
System Data Owner Pat Ahlborn	Patricia H Ahlborn	9/21/06	✓			
Reviewed by OCC Staff Mary Schaffer	Mary Schaffer	9/21/06	✓			
Disclosure Officer Denise Hofmann	Denise Hofmann	9-15-06	✓			
CIO - After approval, distribute to the following:	Kimberly A McCoy (acting)	9-27-06	✓			
E-Commerce Staff Mgr. (OIT) - Post to Privacy Web-Page.	SUBMITTED FOR POSTING	9/28/06				
Date PIA Delivered to OMB Director	SUBMITTED TO OMB	9/28/06				
DIRECTIVES CONTROL POINT CLEARANCE						
APPROVED (Title) CIO			AFTER APPROVAL RETURN TO			