Bureau of the
Public Debt
United States Department of the Treasury

Do Not Pay

Privacy Impact Assessment (PIA)

June 15, 2012

System Information

Name of System, Project or Program: Do Not Pay
OMB Unique Identifier: 015-35-01-01-1039-00

Contact Information

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

   Alexander Dashevsky
   Management and Program Analyst
   Bureau of the Public Debt
   Phone: 202-504-3521
   Email: Alexander.Dashevsky@bpd.treas.gov
   799 9th Street NW
   Washington, DC 20239

2. **Who is the system owner? (Authorizing Official Name, title, organization, phone, email, address).**

   Dara Seaman
   Assistant Commissioner
   Bureau of the Public Debt
   Phone: 202-504-3500
   Email: Dara.Seaman@bpd.treas.gov
   799 9th Street NW
   Washington, DC 20239

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

   Tom Vannoy
   Do Not Pay Program Manager
   Bureau of the Public Debt
   Phone: 202-504-3530
   Email: Thomas.Vannoy@bpd.treas.gov
   799 9th Street NW
   Washington, DC 20239

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

   David Ambrose
   Chief Information Security Officer
   Privacy Officer
   Financial Management Service &
   Bureau of the Public Debt
   Phone: 202-874-6488
   Email: David.Ambrose@fms.treas.gov
   3700 East-West Highway
   Hyattsville, MD 20782

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

   Kimberly A. McCoy
   Assistant Commissioner
   Office of Information Technology
   Phone: 304-480-6635
   Email: Kim.McCoy@bpd.treas.gov
   200 Third Street
   Parkersburg, WV 26106

System Application/General Information

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

   Yes.

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

   The Department of the Treasury's Do Not Pay program is designed to reduce improper payments by facilitating paying agencies (National, State, or Local Governments disbursing federal funds) access to critical information to identify and prevent improper payments.

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

   Executive Order - *Reducing Improper Payments and Eliminating Waste in Federal Programs*, dated November 2009; Presidential Memorandum – *Enhancing Payment Accuracy Through a "Do Not Pay List"*, dated June 18, 2010, and the *Improper Payments Elimination and Recovery Act of 2010*.

The *Consolidated Appropriations Act of 2012* (Public Law 112–74—Dec. 23, 2011) appropriated funds to the Bureau of the Public Debt to reduce improper payments. On April 12, 2012, the Office of Management and Budget (OMB) issued Memorandum M-12-11 - *Reducing Improper Payments through the "Do Not Pay List"*, which directs agencies to develop plans for using the Do Not Pay solution in the Fiscal Service for pre-payment eligibility reviews.

4. **Under which Privacy Act System of Records Notice (SORN) does the system operate? (Provide the system name and unique system identifier).**

   The Do Not Pay program is not a new collection of information. It is operated as a portal and relies on information and data collected by the source agencies. Do Not Pay does not maintain any SORNs of its own in the operation of the program. To the extent that Do Not Pay assists agencies to avoid making improper payments, Do Not Pay relies on any source agency SORNs that may apply.

Data in the System

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

   Categories of individuals include publically available information (i.e., bankruptcy data), those who are deceased, owe delinquent Federal non-tax debt, registered as contractors, debarred from benefitting from Federal programs or contracts, or receive payments funded by the Federal government for any reason.

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?

   Information is not received directly from individuals. Do Not Pay is a portal that provides information collected previously from source agencies or publicly available information.

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

   - Social Security Administration (SSA)
   - General Services Administration (GSA)
   - Department of Treasury (Treasury)
   - Department of Health and Human Services (DHHS).

   Additional data sources are constantly being added by Do Not Pay.

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

None.

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

Public and commercial sources available on the Internet or purchased via third-party providers, and potentially others not yet identified.

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

None.

3. **Accuracy, Timelines, and Reliability.**

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

Customer agencies using the Do Not Pay application will be required to independently verify information provided by Do Not Pay before taking any action. This requirement will be communicated to the customer as part of the on-boarding process.

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

The completeness of the result for each data load process will be validated in a test environment before being used in production. Some or all of the incoming data sets may be periodically replaced entirely.

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).**

The data will be updated with information provided by the source on a scheduled basis, with the frequency for each data source to be determined on a case-by-case basis. The source data owner will be relied upon to maintain and provide current data.

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

The data owner for each source is responsible for maintaining data element descriptions.

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?**

   Yes.

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?**

   No. Data is not aggregated.

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

   No.

4. **Can the system make determinations about employees/public that would not be possible without the new data?**

   No.

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

   The system will not derive new data. However, to the extent that new data is added to the system, the new data will be verified by system testing and independent verification by the paying agency prior to taking any action affecting an individual's eligibility for a Federal benefit or payment. At this time, customers will be Federal and state agencies administering federally funded benefit programs.

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

   The new data is not being consolidated with existing 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 will provide a single point of access to data provided from multiple sources. In addition to common controls in the infrastructure, access controls will be built into the application. Role based application controls will limit access to authorized data.

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.**

   Data is retrieved by any field which includes for example, name (individual or business), social security number/tax identification number, Data Universal Numbering System (DUNS), and address.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   Reports will be defined to provide data necessary to support the system objective to reduce improper payments. Authorized users will use the reports to identify payments that will be investigated further by the customer agency to determine if the past or pending payment may be improper. Upon the paying agency's independent determination of an improper payment, the customer may at its discretion stop a pending payment or pursue recovery of a past payment.

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?**

   Production system components will not be replicated at more than one site.

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

   Source data and data received from customers will be stored in accordance with the commitments made in the data exchange agreement, computer matching agreement, and/or memorandum of understanding with the respective data source provider or customer agency. Reports from the system will be sent to the paying agency that will maintain the data in conformity with the source SORN. The paying agency will maintain the data for such time as is necessary to protect the paying agency's legal rights and interest, or otherwise until they are no longer historically significant.

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?**

   See the response to question number two above. Data and reports will be purged from the retention space (online and/or offline databases and activity logs) in accordance with documented retention requirements established and approved by the National Archives and Records Administration (NARA). The documentation will be maintained by program staff and distributed to system administrators through procedural documentation.

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

   No.

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

   Not applicable.

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

   The data may be used to identify individuals through analytics that will highlight potential aliases, relationships, and identification anomalies for further research. Geographic information (e.g., home and business addresses) may be used to locate individuals for the purpose of debt recovery. The system will not be used to monitor individuals.

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

   The system will not be used to monitor individuals.

8. **What controls will be used to prevent unauthorized monitoring?**

   The system will not be used to monitor individuals.

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

   The Bureau of the Public Debt's Privacy Act Officer will work with data owners to identify revisions required to SORN routine uses. Required revisions will be published in the Federal Register prior to inclusion of the data in the Do Not Pay system.

Access to Data

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

   Public Debt program and support personnel, business partner personnel (i.e., the Federal Reserve Banks of Kansas City and St. Louis), authorized customer personnel, and contractors representing any of these.

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

   Role based application controls will limit user access to authorized data. Program staff will maintain documentation of system access and authorization procedures.

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

   Access will be restricted with role based application controls.

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).**

   Public Debt has implemented suitable system, personnel, and physical security measures to adequately protect the confidentiality and integrity of the information in the system. Public Debt and the Federal Reserve Bank staff are subject to Federal privacy training requirements and must complete Treasury Privacy training that addresses proper identification and protection of data. All data viewed is logged for all users. Users acknowledge that they must comply with any restrictions that apply to the use and disclosure of data they access, including any restrictions that may apply under the Privacy Act.

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?**

   Yes. There are Public Debt and Federal Reserve Bank contractors involved in the system design and development. Privacy requirements were considered in contracts and contractors are required to have the same background checks and Privacy Training as Public Debt and Federal Reserve Bank staff.

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

   Yes. Do Not Pay receives data from the Social Security Administration, General Services Administration, Department of Health and Human Services, Office of the Inspector General, and the Department of Treasury's Financial Management Service.

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

   The Do Not Pay Program Manager will have primary responsibility for coordinating the protection of privacy rights.

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

   Yes.

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

   The data will be used to help prevent and reduce improper payments within the grants, benefits, and contracting communities.

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

    The Do Not Pay Program Manager will have primary responsibility for assuring the data is properly used within the Do Not Pay Program. An internal control and compliance program will be in place to ensure correct procedures are followed and that only appropriate data disclosures are made by the program in general or by specific applications developed by the program. Do Not Pay has been through the Security Assessment and Authorization process and been authorized to operate.

    Proper use of the data in Do Not Pay is a shared responsibility between the Do Not Pay program manager and the customer agencies of any application the program develops. Customer agencies are responsible for ensuring only authorized users with appropriate routine uses are enrolled as users and are responsible for ensuring any data displayed after performing a search is appropriately maintained, controlled, and protected.