The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):
http://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Treasury’s Working System
Document Version: 2.0
Document Date: 05/14/2015

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.
Treasury’s Working System was established to serve as a “single point of entry” through which agencies access relevant data in order to determine eligibility for a Federal award or payment.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

TREASURY/Fiscal Service .023 - Do Not Pay Payment Verification Records

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

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

a. Is the information about members of the public?
Yes, but DNP does not collect the information directly from members of the public. It maintains individual information disclosed from other federal agencies (as approved by OMB) as required under the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA).

b. Is the information about employees or contractors?
Yes, agencies may use information from Treasury’s Working System to verify eligibility of a contractor or other recipient of Federal payments at various times during the payment cycle, most significantly pre-award and prepayment.

5) What legal authority authorizes the purchase or development of this system?
Improper Payments Elimination and Recovery Improvement Act of 2012, 31 U.S.C. 3321 note, Public Law 112–248; The Improper Payments Elimination and Recovery Act of 2010, Public Law 111–204; E.O. 13520 (Reducing Improper Payments and Eliminating Waste in Federal Programs), 74 FR 62201; OMB Memorandum M–13–20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative); Presidential Memorandum on Enhancing Payment Accuracy through a ‘‘Do Not Pay List’’ (June 18, 2010).

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:
__ Employees

X Contractors
X Taxpayers
Others (describe)

2) Identify the sources of information in the system
Check all that apply:
__ Employee
__ Public
X Federal agencies
__ State and local agencies
X Third party

a. What information will be collected from employees or contractors?
None. DNP does not collect information directly from contractors.

b. What information will be collected from the public?
None. DNP does not collect information directly from members of the public.

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

1. Death Master File (DMF), Social Security Administration (SSA)
2. SAM Exclusion Records, General Services Administration (GSA)
3. Treasury Offset Program (TOP) Debt Check[1], Department of the Treasury
4. List of Excluded Individuals/Entities (LEIS), Health and Human Services (HHS)
5. Credit Alert System or Credit Alert Interactive Voice Response Systems (CAIVRS), Department of Housing and Urban Development (HUD)
   a) In addition to HUD's data, CAIVRS is comprised of data from the Department of Education, Department of Justice (DOJ), U.S. Department of Agriculture (USDA), Veterans Affairs (VA) and the Small Business Administration (SBA)
6. Prisoner Information, SSA
7. Additional agencies as designated by the Office of Management and Budget (OMB), in accordance with the process outlined in OMB M-13-20. Please see response to (e) below for additional details.

d. What state and local agencies are providing data for use in the system?
None. DNP does not collect data directly from state or local agencies.

e. From what other third party sources will data be collected?
Presently, OMB has not designated any commercial data sources for Treasury's Working System. As commercial data sources are considered, DNP will prepare and submit to OMB a written assessment to document the suitability of the commercial data source. The assessment will explain the need to use or access the data, explain how the data will be used or accessed, provide a description of the data (including each data element that will be used or accessed), and explain how the data source meets all applicable requirements of OMB M-13-20. OMB will provide the written assessment to the public as part of a notice in the Federal

[1] Referred to as Debt Check Database in IPERIA

Register for a 30 day comment period. At the conclusion of the 30-day comment period, if OMB decides to finalize the designation, OMB will publish a notice in the Federal Register to officially designate the data source for inclusion in Treasury's Working System.

3) Accuracy, Timeliness, and Reliability

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

The two measures of Accuracy listed below are used to determine the correctness of the data presented in the data source being evaluated.

Metric	Definition
Concordance	The quantity of values that are correct with regard to a gold standard
Consistency	The quantity of values that follow known logical relationships between data elements

b. How will data be checked for completeness?

The two measures of Completeness listed below are used to determine the overall proportion of the data which contains the required attributes.

Metric	Definition
Schema (%)	Percentage of required data elements present in the data source
Record (%)	Percentage of records containing legitimate, non-null/non-blank values for all required data elements

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

There are five Freshness measures which
1) help to evaluate whether a data source is up-to-date/current, and
2) set the time expectation for the availability of information. These measures are listed below.

Metric	Definition
Currency	Data update / refresh frequency
Availability	Average length of time between data record acquisition by the provider and analyst access to the data
Latency	Median length of time between the original event and the acquisition of a record describing the event by the data source
Timeliness	Maximum length of time between potential data changes and data refresh events
Obsolescence (%)	Percentage of records changed via updates at each refresh

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

Please see Categories of Records in the System section of the Department of the Treasury/Bureau of the Fiscal Service .023 – Do Not Pay Payment Verification

Records – System of Records Notice, available at:
http://donotpay.treas.gov/Privacy.htm

ATTRIBUTES OF THE DATA:

1) How is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Treasury's Working System provides authorized agencies with information about intended and actual payees of Federal funds in two ways. First, the Treasury's Working System enables authorized Federal agencies to access information from multiple databases through a central web portal maintained by DNP. Second, DNP compares information about payees from payment files submitted by Federal paying agencies to information contained in multiple data sources. For both methods, the paying agency reviews any data provided by Treasury's Working System to determine whether the data are correct and how the data impacts payment eligibility in accordance with program-specific eligibility rules and procedures. In addition, DNP provides data analysis that helps agencies detect fraud and improve internal controls to systemically prevent, identify, and recover improper payments.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?

Treasury's Working System includes activities such as investigation activities for fraud and systemic improper payments detection through analytic technologies and other techniques. This may result in the creation of new data or previously unavailable data about an individual. Records in this system created or collected by DNP are governed by a National Archives and Records Administration (NARA) records schedule, and are generally retained for a maximum of seven years after the end of the fiscal year in which the record was created. Pursuant to Section 7(b) of OMB M 13–20, DNP will retain and dispose of records supplied by other Federal agencies in accordance with our written agreements with those agencies.

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

The new information may be linked to an individual's record.

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

No, the system does not make determinations about members of the public. Before adverse action is taken against an individual, however, any adverse information that agencies discover shall be subjected to investigation and verification, unless an agency's DIB waives this requirement pursuant to the Privacy Act at 5 U.S.C. § 552a(p)(l)(A)(ii). Verification requires a confirmation of the specific information that would be used as the basis for an adverse action against an individual. As explained in OMB guidance, "Absolute confirmation is not required; a reasonable verification process that yields confirmatory data will provide the agency with a reasonable basis for taking action." In each case, agencies shall document the specific information on which any determination about an individual is based.

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

DNP will follow procedures for the accuracy and correction of information in the system described in OMB M–13–20, available at:
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-20.pdf

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
Data is not being consolidated.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?
Processes are not being consolidated.

8) How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)
Records may be retrieved by identifiers, including, but not limited to, exact name, partial name, social security number (SSN), Taxpayer Identification Number (TIN), Employer Identification Number (EIN), Data Universal Numbering System (DUNS) numbers, or a combination of these elements.

9) What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
Payment issuing agencies will have access to reports on individuals to support determinations about the disbursement of payments or awards, consistent with legal authority. Only authorized Federal agency personnel with appropriate security credentials may access the data available.

10) What opportunities do individuals have to decline to provide information (i.e., in such cases where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)? How can individuals grant consent?
Information is not provided voluntarily and the uses of the information are dictated by the routine uses for the applicable systems of records.

<u>MAINTENANCE AND ADMINISTRATIVE CONTROLS:</u>

1) What are the retention periods of data in this system? How long will the reports produced be kept?
Records and reports from this system are generally retained for a maximum of seven years after the end of the fiscal year in which they were created. Pursuant to Section 7(b) of OMB M-13–20, DNP will retain and dispose of records supplied by other Federal agencies in accordance with DNP's written agreements with those agencies.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?
Pursuant to Section 7(b) of OMB M-13–20, DNP will retain and dispose of records supplied by other Federal agencies in accordance with our written agreements with those agencies. Those disposition procedures are documented in Memoranda of Understanding (MOU) with original data source agencies and/ the SORN(s) that corresponds.

3) If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?

The consistent use of the system will be maintained in accordance with Treasury's Working System foundational documents to include, but not limited to:

- Data Management Plan
- Agency Implementation Guide
- Concept of Operations (ConOps)
- Data Correction Process Standard Operating Procedures (SOP)

4) Is the system using technologies in ways that Fiscal Service has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?
N/A because the system is not using technologies in ways that Fiscal Service has not previously employed.

5) How does the use of this technology affect employee or public privacy?
N/A. Please see response to number 4 above.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
Yes, Treasury's Working System will provide that capability since it may contain the following information:

a) Name(s), including aliases, and surnames;
b) Date of birth;
c) Home and work address;
d) Driver's license information and other information about licenses issue to an individual by a governmental entity;
e) Home, work, and mobile telephone numbers;

This information, however, will not be used for purposes other than to assist Federal agencies in verifying that individuals are eligible to receive Federal payments, as required by IPERIA.

7) What kind of information is collected as a function of the monitoring of individuals?
None.

8) What controls will be used to prevent unauthorized monitoring?
Internal access log control measures are reviewed to ensure compliance with security guidelines governing access to Privacy Act data.

ACCESS TO DATA:

1) Who will have access to the data in the system?
Check all that apply:

X Contractors
X Users
__ Managers
X System Administrators
__ System Developers
__ Others (explain)_________

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

Access to this system is determined through an extensive onboarding process to ensure access to the data being requested is in line with the objectives for which this system was developed and it directly supports program integrity efforts of the agency to reduce improper payments. The requesting agency is required to fill out a questionnaire to ensure the privacy of individuals is safeguarded and in compliance with all applicable requirements, constraints and privileges under the Privacy Act, applicable laws, regulations, policies, Computer Matching Agreements (CMAs), and MOUs governing the use of records in this system. Once approved, the use of two factor authentication and role based application controls will ensure access to data by system users aligns to that for which the user/agency has been granted access to. 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 to computerized records is limited through the use of internal mechanisms available to only those whose official duties require access.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Audit logs allow system managers to monitor external and internal user actions and address any misuse or violation of access privileges. Rules of Behavior clearly document what constitutes unauthorized behavior. Users are required to sign these rules prior to gaining access to the system. Annual Privacy and Information Security Awareness training is also required of all Treasury personnel.

5) If contractors are/will be involved with the design, development or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?

Contractors are required to have the same background checks and privacy training as DNP and Federal Reserve Bank (FRB) staff.

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

__yes
X no

If yes,

a. Explain the interface.

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

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

X yes
__no

If yes,

a. Check all that apply:

X Federal

__State
__ Local
__Other (explain) __________________

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

The system enables programs of executive agencies to review records that assist them in identifying, preventing, and recovering payment error, waste, fraud, and abuse within federal spending as required by IPERIA.

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

Only authorized Federal agency personnel with appropriate security credentials may access the data available through Treasury's Working System.