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/fspia/fs_pia.htm

Name of Service: Digital Pay Pilot Service (formerly NTAP)

Document Version: 3.0

Document Date: March 6, 2017

SYSTEM GENERAL INFORMATION:

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

   The Digital Pay Pilot Service (formerly NTAP) facilitates the disbursement of payments utilizing online payment networks. Payments are initiated using an email address or cell phone number and utilizes the ACH and debit card payments infrastructure. Digital Pay provides Federal agencies another electronic alternative to paper checks for disbursement of payments.

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

   FMS .002 Payment 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

   b. Is the information about employees or contractors?

   Yes – Federal Employees

5) **What legal authority authorizes the purchase or development of this system?**

   5 U.S.C. § 552a; 31 U.S.C. §§ 3332(g), 3321, 3325; 31 CFR Part 208

DATA in the SYSTEM:

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

__ **Taxpayers**
_X_ **Others (describe)** to include members of the public.

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

a. **What information will be collected from employees or contractors?**

The service will collect first and last names, business email addresses, business phone numbers.

b. **What information will be collected from the public?**

The service will collect first and last names, personal email addresses, and personal phone numbers.

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

Department of Justice; U.S. Marshals Service

d. **What state and local agencies are providing data for use in the system?**

None

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

None

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

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

Payment data comes from a Federal Program Agency (FPA) certifying agency. The FPA certifies the payment request to the Fiscal Service, and the FPA is responsible for the accuracy of the payment data submitted.

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

The FPA certifies data for completeness.

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

The FPA certifying process helps to ensure the data is current.

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

The data elements are described in the Digital Pay Data Field document.

ATTRIBUTES OF THE DATA:

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

The use of data is relevant and necessary to properly process payment requests from a certifying FPA by accurately controlling which users initiate payments, approve payments, receive payments, and otherwise ensures payments are disbursed in the correct amount. This process is consistent with the purpose of the system to facilitate the accurate and timely disbursement of Federal monies.

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?**

No

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

No

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

No

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

No new data will be placed in the individual's record.

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

All data collected in Digital Pay is protected utilizing strong encryption methods.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

Yes, access controls within the system are role-based.

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 are not searchable by personal identifying information. Reports can be generated using batch report schedule number and by date. These reports include first and last names, email addresses and phone numbers.

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

No reports can be produced on individuals. However, reports can be generated using batch report schedule number and by date. The Digital Pay FPA reporting users are the only ones capable of generating this report.

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?**

Participation is voluntary.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

1. Payment records are retained for 7 years.
2. System Reports (Ad Hoc and Data File Outputs) are retained in accordance with GRS 4.3, Items 030/031 whose disposition instructions read "Destroy when business use ceases".

   Note: Excluded are all copies (paper and electronic) of Tribal Trust Litigation payment records which are currently under a records legal hold and must be preserved indefinitely until case is settled.

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

Excluding Tribal Trust Litigation records, disposition instructions and authority follow:

Temporary: Cut off at end of fiscal year. Delete / destroy 7 years after cutoff. (N1-425-09-5, Collections, Payments and Claims, Item 2, Federal Program Agency (FPA) Operation Records).

Disposition procedures are documented and approved by the Bureau of the Fiscal Service Records Management Branch.

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?**

   Replication is used to ensure consistent use of the system and data at all sites.

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

   Yes, the system is utilizing online payment networks for disbursement of payments.

5) **How does the use of this technology affect employee or public privacy?**

   N/A

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

   No

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?**

   Industry best practices for firewalling; perimeter protection and system monitoring are employed. Users are required to sign Rules of Behavior (ROB), vendors are required to sign Non-Disclosure Agreements (NDA). Periodic reviews will be performed to prevent unauthorized monitoring.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   _X_ Contractors
   ____Users
   _X_ Managers (Certifying Officer)
   _X_ System Administrators
   _X_ System Developers
   _X_ Others (explain) - Treasury authorized users to verify and certify payment.

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

   Access to data is granted by roles. The Federal agency designated Account Manager is primarily responsible for the determination and management of the agency's user access in the Digital Pay Service Pilot portal and the agency's data.

Privilege user accounts are only granted to perform specific procedures and restricted to specific roles and responsibilities.

Audit logs of authentication and provisioning events are recorded.

All contractor employees working with the Digital Pay undergo a background investigation, signs Rules of Behavior and Non-Disclosure Agreements (NDAs), and are all subject to personnel security requirements.

A procedure for USMS provisioning and user access request is documented. User access requests are only approved by appropriate USMS personnel prior to granting access. Criteria, procedures, and controls are documented.

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

Users access will be restricted to specific roles, responsibilities, and data.

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)**

Access to data is granted by roles. Audit logs of authentication and provisioning events are recorded. Periodic reviews will be performed to prevent unauthorized monitoring.

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?**

Yes, Privacy Act contract clauses were inserted into contracts.

6) **Do other systems share data or have access to the data in the system?**
__ yes
_X_ no

If yes,

a. Explain the interface.

N/A

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

N/A

7) **Will other agencies share data or have access to the data in this system?**
__ yes
_X_ no

If yes,

a. Check all that apply:

__Federal
__State
__ Local
__Other (explain) _____

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

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