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: Post Payment System

Document Version: 3.0

Document Date: 8/28/2017

SYSTEM GENERAL INFORMATION:

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

The Post Payment System (PPS) will consolidate all payment aftermath processing into one comprehensive application by consolidating processing currently performed in five (5) legacy post payment systems. PPS uses standardized reporting structure and leverage Commercial-off-The-Shelf (COTS) software solutions when feasible to provide common, best practice functionality and proven implementation methodologies.

Processes to be included in PPS are:

- Payment Matching and Verification
- Returns and Cancellations
- Inquiries and Claims
- Research and Reclamations
- Fraud Detection and Analysis
- Accounting and Reconciliation
- Reporting and Analysis
- Customer Portal

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

FMS .002 Payment Records
FMS .003 Claims and Inquiries on Treasury Checks and International Claimants
FMS .006 Direct Deposit Enrollment Records
FMS .014 Debt Collection Operating System

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, but only in as much as they are payees of the U.S. Treasury. The information for PPS is received from the Payment Automation Manager (PAM) System, Automated

Standard Application for Payments (ASAP), International Treasury Services (ITS), Payments Accounting Claims Enhanced Reconciliation (PACER), Treasury Check Information System (TCIS), and the Federal Reserve Automated Clearinghouse (FedACH).

5) What legal authority authorizes the purchase or development of this system?
The following: (31 U.S.C. 321, 3301, 3325, 3327, 3328, and 3334) give the Bureau of the Fiscal Service and the Secretary of the Treasury the legal authority and authorization for the development of the Post Payment System (PPS).

Under 31 U.S.C. 321(a) The Secretary of the Treasury shall - (1) prepare plans for improving and managing receipts of the United States Government and managing the public debt; (2) carry out services related to finances that the Secretary is required to perform; (3) issue warrants for money drawn on the Treasury consistent with appropriations; (5)prescribe regulations that the Secretary considers best calculated to promote the public convenience and security, and to protect the Government and individuals from fraud and loss, that apply to anyone who may: (A) receive for the Government, Treasury notes, United States notes, or other Government securities; or (B) be engaged or employed in preparing and issuing those notes or securities.

Under 31 U.S.C. Sec. 3301, General duties of the Secretary of the Treasury are described:
(a) The Secretary of the Treasury shall -
(1) Receive and keep public money;
(2) Take receipts for money paid out by the Secretary;
(3) Give receipts for money deposited in the Treasury;
(4) Endorse warrants for receipts for money deposited in the Treasury;
(5) Submit the accounts of the Secretary to the Comptroller General every 3 months, or more often if required by the Comptroller General; and
(6) Submit to inspection at any time by the Comptroller General of money in the possession of the Secretary.

The following sections authorize:
3325. Vouchers.
3326. Waiver of requirements for warrants and advances.
3327. General authority to issue checks and other drafts.
3328. Paying checks and drafts.
3334. Cancellation and proceeds distribution of Treasury Checks

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   X Employees
   X Contractors
   X Taxpayers
   X Others (describe)
   Any payee associated with receiving a Treasury payment, letter, and/or supporting documentation.
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?
Post Payment System (PPS) does not collect any PII information directly from taxpayers, employees, contractors, or other payees of Federal payments. All PII payment-related information is provided through PAM, ITS, PACER, or TCIS; ASAP from recipient-initiated payment services; and the FedACH.

b. What information will be collected from the public?
Post Payment System (PPS) does not collect any PII information directly from the public. All PII payment-related information is provided through PAM, ITS, PACER, or TCIS; ASAP from recipient-initiated payment services; or the FedACH.

c. What Federal agencies are providing data for use in the system?
All Federal Program Agencies (FPAs) that authorize and certify benefit, salary, vendor, and other payments to be disbursed by the Department of the Treasury and Non-Treasury Disbursing Offices (NTDOs).

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?
Automated Clearinghouse (ACH) payment information (Enrollment Requests (ENRs), Notifications of Change (NOCs), pre-notifications, and IRS ACH returned payments from Financial Institutions (FIs) via the FedACH.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources, other than Fiscal Service records, be verified for accuracy?
Automated PII validation processes ensure that required fields and records in incoming data are filled according to rules established by Fiscal Service and agreed upon by originating agencies and financial institutions.

b. How will data be checked for completeness?
Automated PII validation processes ensure that required fields and records in incoming data are filled according to rules established by Fiscal Service and agreed upon by originating agencies and financial institutions.

c. What steps or procedures are taken to ensure the data is current?
All payment and collection PII information received by PPS from PAM, ITS, ASAP, PACER, TCIS, or the FedACH goes through internal control and validation checks by the sending system or organization. PPS relies on the sender for prior PII data validation.

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

The PII data elements are described in the PPS Data Dictionary/Data Model. They are also described in input and output file specifications.

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?**
   All PII information collected and disseminated is relevant and necessary for the Fiscal Service to fulfill its lawful mission. Fiscal Service is responsible for all record keeping of disbursements and collections made by Treasury Disbursing Offices (TDOs), the Debt Management System (DMS), Automated Standard Application for Payments (ASAP), and International Treasury Services (ITS). Fiscal Service is also responsible for reconcilement of all U.S. Treasury checks disbursed world-wide, customer inquiries, and the adjudication of all claims made against disbursed payments. Access to PII data is also needed to ensure compliance with Federal security laws and regulations.
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?**
   PPS will derive new data or create previously unavailable data about an individual through aggregation from the information collected for fraud detection purposes. The fraud detection data will be stored in PPS databases that have IT controls in place to limit unauthorized access.
3) **Will the new data be placed in the individual's record?**
   Yes**.**
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?**
   Authorized employees will contact the program agency with suspect information to have the program agency determine if fraud has occurred. Further action will be taken based on the business agreements between the program agency and Fiscal Service.
6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
   Consolidated data is stored in the PPS databases that have IT controls in place for limiting unauthorized access. Data will be retained in PPS primarily for payment reconciliation, inquiries, claims adjudication, and fraud detection purposes. PII data related to the administrative management of PPS may also be consolidated. Such information may be made available by the PPS System Owner, or designee, as needed to investigate improvements, security breaches, or possible error resolution.

   The PPS database is encrypted with approved FIPS 140-2 cryptographic modules to secure data from unauthorized access.

   The PPS database servers are located behind and secured with active Intrusion Detection Systems and firewalls.

   Data from other sources are sent via encrypted channels from other agencies and systems to the PPS file servers.

Privileged accounts such as database administrators are granted only after specific approvals using formal procedures enforcing the concept of least privilege determined by the privileged user's job functions and responsibilities.

Users from specific agencies can only view financial data that is specifically issued by their respective agencies (e.g. IRS user cannot see SSA claims, returns, reclamations).

Treasury users may be able to access all the financial data from PPS as determined by their job function and responsibilities.

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

   All access to consolidated PII data is subject to the same controls as set out above. Users are restricted to view data that they have been authorized to access through user provisioning and PPS access controls.

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.)**

   Data from PPS is generally retrieved by Payee ID, name, mailing address, FI routing and transit number (RTN) and FI account number for fraud detection purposes. Fiscal Service employees can access data by Payee ID based on their defined role(s). Data can also be retrieved by check symbol/serial number or ACH trace number/date of payment (both are non-personal identifiers).

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

   PPS can provide reports based on Payee ID, name, mailing address, FI routing and transit number (RTN) and FI account number for fraud detection purposes. Reports are created when possible payment fraud is detected. These reports will be provided to those program agencies participating in the fraud detection process. Fiscal Service employees and Agency personnel authorizing the payments will have access to these reports.

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?**

    Under PPS, individuals will have no opportunity to decline to provide information.

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. Direct deposit enrollment records are retained for 7 years.
   3. 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 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:

Cut off at the end of the fiscal year in which action on a debt, collection, payment, claim or other item is completed. Delete / destroy 7 years after cutoff. (N1-425-09-5, Collections, Payments and Claims, Item 2, FPA Operation Records and N1-425-09-1, Debt Collection, Item 2, Federal Program Agency Operations Records).

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?**

PPS will primarily operate from one site and all users run the same version of the application. Fiscal Service configuration management procedures permit only one version to be in production at any given time. Data will be replicated to the PPS contingency site by database replication or restoring data from backup tapes. The contingency site will only be used in when the primary site is not operational and only one site will operate at any given time.

4) **Is the system using technologies in ways that Fiscal Service has not previously employed**

(e.g., monitoring software, Smart Cards, Caller-ID)?

No.

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.**

Yes.

The individual information in PPS is static information related to the issuance of payments, debt collection, or fraud detection. Certain personal information (e.g.; payee ID, name and address, FI RTN and account number, and payment type) may also be used in various payment aftermath processes.

For administrative and audit purposes, the system retains information related to the identity of employees that have made changes or completed processes within the system in the normal course of business.

7) **What kind of information is collected as a function of the monitoring of individuals?**

Payee ID, name and address, FI RTN and account number will be used to monitor possible fraud activities (e.g., type and pattern of payment delivery). Fiscal Service employees accessing PPS will be monitored by their system User ID.

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

Information in PPS is available to Fiscal Service employees, and contractors; external federal agencies' employees and contractors; and FRB personnel according to the authorities granted and in accordance with the Fiscal Service Baseline Security Requirements (BLSRs): AC-2 Account Management. Employees, contractors, and FRB personnel are counseled that they may only view information available to them on a "need-to-know" basis in the performance of their duties and sign a "Rules of Behavior".

ACCESS TO DATA:

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

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

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

Fiscal Service is responsible for final approval of user accounts. All access requests are documented within an access control/provisioning system. All requests include a user role and specify what agency data will be accessed. User accounts are approved by the user's supervisor who validates the need for access and finally the PPS Information System Security Officer.

User provisioning is documented in a user enrollment guide that includes procedures and responsibilities. A PPS security matrix and system security plan documents the controls for access.

Privileged user accounts such as ones for database administrators are granted only after specific approvals using formal procedures enforcing the concept of least privilege determined by the privileged user's job functions and responsibilities.

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

Fiscal Service users have access to that data and those actions needed in the normal performance of their duties. Certain actions will be limited to appropriate manager/supervisors in Fiscal Service.

PPS database administrators have access to database information. Program managers at Fiscal Service, Federal Reserve Bank (FRB), and Treasury Web Applications Infrastructure (TWAI) as well as system administrators (including the PPS application information system security officer, FRB personnel, and TWAI personnel) will have access to audit logs of actions taken within the system. This is required for monitoring unauthorized access and/or use of the system.

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)**

All Fiscal Service personnel must take a mandatory annual Cyber Security and Privacy Awareness training courses. This training includes a review of selected security procedures and Privacy Act information. All personnel associated with PPS must agree to the "Rules of Behavior" document prior to obtaining system access. Those agreeing to the Rules of Behavior signify that they understand the information technology (IT) security and privacy requirements, accept the IT security and privacy requirements, and acknowledge that disciplinary action may be taken based on violation of the Rules of Behavior. It applies to all Fiscal Service employees,

contractors, fiscal agents, financial agents, and subcontractor personnel who access IT systems and the facilities where Fiscal Service information is processed, transmitted, and stored as well as to all physical space housing IT systems, communications equipment, and supporting environmental control infrastructure that impact IT areas.

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.
6) **Do other systems share data or have access to the data in the system?**
   X yes
   __no

   If yes,

   a. Explain the interface.
   Data is received via secure channels from other systems to the PPS file servers. Sources include PAM, TCS, TRACS, PACER, PIR and TCIS, ASAP and ITS.

   b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.
   The Fiscal Service Chief Privacy Officer and the PPS Authorizing Official.

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.
   Personnel associated with other federal agencies also have access to information for their particular agency. The information of one agency (or subset thereof) may not be viewed by another agency (or subset thereof).
   It should be noted that much of the information within the system is often that which was originated by the federal agencies and is resident in their systems. Data is normally only disclosed to those agencies that originated payments that led to reconcilement and adjudication information. Any other disclosures will be made only in accordance with the provisions of 26 USC 6103 (restricting the disclosure of tax return information), 5 USC 552a (the Privacy Act) and 18 USC 1905 (the Trade Secrets Act), and other applicable laws and will be made using the procedures outlined above.

   c. Identify the role responsible for assuring proper use of the data.
   The PPS system owner has responsibility for ensuring compliance.