



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: Payment Automation Manager (PAM)

Document Version: 1.1

Document Date: March 16, 2016

SYSTEM GENERAL INFORMATION:

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

PAM is the next generation Payment System which accepts, validates, and certifies payment requests and issues ACH, check, and wire disbursements for almost all Federal Program Agencies. These disbursements range from benefits payments (e.g. SSA retirement and disability benefits, OPM Federal retirement), IRS tax refunds, Federal salaries, and vendor and miscellaneous payments. The end state product will be a standardized system that is extendible and highly configurable.

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

PAM does not use personal identifiers to retrieve records, it does not require a SORN.

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

yes, explain.
 no

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

yes
 no

a. Is the information about members of the public?

Yes, the system contains certain Vendor/Miscellaneous/Salary, SSA, SSI Daily payment information for members of the public.

b. Is the information about employees or contractors?

Yes, the system contains certain Salary and Travel Daily payment information for government employees.

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

31 USC 3325

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Check all that apply:

- Employees**
- Contractors**
- Taxpayers**
- Others (describe)**

2) Identify the sources of information in the system

Check all that apply:

- Employee**
- Public**
- Federal agencies**
- State and local agencies**
- Third party**

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

The system contains certain Salary and Travel Daily payment information for government employees.

b. What information will be collected from the public?

The system contains certain Vendor/Miscellaneous/Salary, SSA, SSI Daily payment information for members of the public.

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

PAM will disburse payments (Automated Clearing House (ACH), checks, and wire transfers) on behalf of virtually every Federal agency in the Executive Branch, except for most Department of Defense and certain independent agencies such as the U.S. Postal Service. PAM also disburses for all or some types of payments associated with agencies that possess statutory or delegated disbursing authority (e.g., Dept. of Defense, U.S. Postal Service, U.S. Courts, etc.).

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 Federal Program Agencies (FPAs). Each FPA is responsible for the accuracy of the payment data submitted. Fiscal Service maintains no files as to entitlement for any recipient of a payment PAM issues at the request of a FPA.

b. How will data be checked for completeness?

FPA's certify data as complete and accurate. PAM enforces file validation rules based on published formats, which include control records for total payment amount and number of items to be paid. These controls are certified against a summary schedule supplied by the agency via the Secure Payment System.

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

FPA's provide and certify the data PAM receives.

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

PAM Input 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?

Use of the data is relevant and necessary to properly process the payment files from the FPA's for disbursement.

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?

N/A

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

N/A

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

N/A

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

The payment data will be consolidated into one database. No PAM user roles have direct access to the database. All the PII and Sensitive But Unclassified data will be audited. All the access to the database tables that contain PII data is audited and reviewed daily. Access is limited based on the principle of least privilege.

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

There are specific application-defined roles that will execute specific processes within the PAM application.

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.)

Personal identifiers are not used to retrieve information in PAM. PAM is mainly oriented toward the processing of batches of payments and not based on retrieval of individual payments. All retrieval is based on control information.

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

None.

- 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?**

PAM does not collect any information directly from taxpayers, employees, or other payees of Federal payments. All payment-related information is provided by the FPA requesting the payment to be made and is required for accurate issuance of the payment.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

- a. Payment records are retained for 7 years.
- b. 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).

- 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?**

PAM is not operated in more than one site.

- 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.**

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?**

Access to the PAM application will be granted on a “need-to-know” basis. Users, developers and testers receive mandatory annual privacy awareness training. In addition, PAM application users are required to sign Rules of Behavior that include the Privacy Act responsibilities. All PAM Developers receive the same annual training.

All Auditors and 3rd party vendors are required to sign non-disclosure statements that reference the Privacy Act during the Security Assessment process and scans. Periodic Supervisory Reviews will be performed to ensure users are not performing unauthorized monitoring of data. Reports and on-line displays will reference non-disclosure of Privacy Act information.

ACCESS TO DATA:

- 1) **Who will have access to the data in the system?**

Check all that apply:

Contractors

Users (All users are internal Fiscal Service employees).

Managers

System Administrators

System Developers

Others (explain) Database Administrators and Super Programmers

- 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 role and roles are assigned consistent with the principle of least privilege.

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

User access to data will be restricted. Access is granted by role and roles are assigned consistent with the principle of least privilege.

- 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 the PAM application will be granted on a “need-to-know” basis. Users, developers and testers receive mandatory annual privacy awareness training. In addition,

PAM application users are required to sign Rules of Behavior that include the Privacy Act responsibilities. All PAM Developers receive the same annual training.

All Auditors and 3rd party vendors are required to sign non-disclosure statements that reference the Privacy Act during the Security Assessment process and scans. Periodic Supervisory Reviews will be performed to ensure users are not performing unauthorized monitoring of data. Reports and on-line displays will reference non-disclosure of Privacy Act information.

- 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?**

yes

no

If yes,

- a. Explain the interface.**

PAM will push data to interfacing systems. No interfacing systems will access data in PAM.

- 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 PAM Authorizing Official are responsible.

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

yes

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.**

The FPAs send their payment data to PAM for processing. The FPAs only receive the acknowledgement of receipt from PAM.

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

The Chief Information Officer of Fiscal Service and the PAM Authorizing Official are responsible for proper use of the data.