Financial Management Service
Privacy Impact Assessment

Name of Project: Payment Automation Manager (PAM)

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual[1]?
(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Yes

b. Is the information about individual members of the public?
(If YES, a PIA must be submitted with the OMB Exhibit 300 and with the IT Security C&A documentation).

Yes

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the FMS IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, the system contains certain salary and debt collection information as payment data for government employees.

2) What is the purpose of the system/application?

The Financial Management Service (FMS), a bureau of the Department of the Treasury, is responsible for issuance of payments for most Federal Program Agencies (FPAs) of the Federal Government.

The information in PAM relates to payments made on behalf of these FPAs to individuals and business entities. In order for FMS to issue payments on behalf of a federal program agency, detailed information for

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

the payment inscription is required from the agencies. This detailed information includes payee name, a payment amount, address/destination and a payment date.

The PAM project was initiated to standardize and modernize 30+ existing FMS payment applications which generate check and EFT payments on behalf of FPAs. In addition to standardizing the application, the project is also committed to incorporating processing efficiencies and re-engineering processes.

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

31 USC 3325

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

The individuals covered by the system are payees/recipients of US Government payments (e.g., Social Security Administration benefits, Internal Revenue Service Tax refunds, Federal salary, VA Benefits, OPM Annuities, Railroad Retirement Annuities, Vendor and Miscellaneous payments, etc.)

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?

Federal Program Agencies provide all payment data; no data is obtained from the individual.

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

Almost all Federal agencies provide information to FMS to disburse checks on behalf of the Federal government.

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

None.

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

None

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

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.

3) Accuracy, Timeliness, and Reliability

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

Payment data comes only from FPAs. Each FPA is responsible for the accuracy of the payment data submitted. FMS maintains no files as to entitlement for any recipient of a payment FMS issues at the request of a FPA.

b. How will data be checked for completeness?

FPAs 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. 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).

FPAs provide and certify the data received.

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

Yes, the name of the document is Input File Specifications and Outgoing File Specifications.

C. ATTRIBUTES OF THE DATA:

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

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

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

Not applicable

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

Not applicable

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

Not applicable

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. Very few roles will have direct access to the database. Each role will be reviewed to determine if there is a business need to access the database. All privacy and Sensitive But Unclassified data will be logged in a table that will have limited access.

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

There will be specific application-defined roles that will execute specific processes within the PAM application. Access to the database will be restricted.

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.

PAM is mainly oriented toward the processing of batches of payments and not based on retrieval of individual payments. The system will provide limited retrieval based on Name, Account, taxpayer identification number (TIN), social security number (SSN), or bank routing number.

9) **What kinds 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., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can 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.

D. 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?**

   PAM is designed to run at the primary computer site, the back up site, or both at the same time. Data will remain consistent by utilizing mirroring techniques and inter-system communication.

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

   With the exception of a subset of recurring Social Security Administration (SSA) payments, payment details are maintained in the system long enough to recover processing and support agency Business Continuity Plan needs. Summary information, audit information and logs are retained indefinitely.

   SSA recurring payment information is retained on an ongoing basis and is maintained with update information received from SSA.

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?**

   Disposition of data at the end of the retention period will be controlled by the system, returning the space to the operating system.

   Privacy information will not be included in reports.

   Procedures are documented in the system requirements document.

4) **Is the system using technologies in ways that the FMS 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.**

No

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

Not applicable

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 (FMS and Contractors) will receive mandatory annual privacy awareness training. In addition, users (FMS and Contractors) are required to sign Rules of Behavior annually that include the Privacy Act responsibilities. All Auditors and 3rd party vendors are required to sign non disclosure statements that reference the Privacy Act. 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. Certain roles have higher levels of access to the Privacy Act information and these roles have a signed Designation Letter detailing their specific responsibilities.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Treasury/FMS .002 – Payment Issue Records for Regular Recurring Benefit Payments

Treasury/FMS .016 - Payment Issue Records for Other Than Regular Recurring Benefit Payments

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Not applicable, as PAM is a new system that will replace 30+ existing FMS payment applications which generate check and EFT payments on behalf of FPAs.

E. ACCESS TO DATA:

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

All PAM users are internal Financial Management Service (FMS) employees.

The PAM payment processing is done mainly through batch jobs. PAM

access and privileges are based on the user's group assignments or roles and are restricted to the minimum required to perform their job functions. All transactions will be written to a permanent, unalterable audit log, which will include type of transaction, date/time, and the component of the information system where the event occurred, type of event, user identity, the outcome (success or failure) of the event, and the previous and new values modified during the event, if applicable.

Developers will not have access to production PAM payment data and when requiring test data any production data will be sanitized before use.

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

Some FMS users will be able to view payment data for all FPAs. All transactions will be written to a permanent, unalterable audit log, which will include type of transaction, date/time, and user.

Criteria and controls are contained in PAM requirements and architecture/design/development documentation.

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

User access will be defined and controlled by role based security. Users will be assigned access for the level of access needed to perform job duties based on the defined roles.

System Administrators will have access to all payment data in PAM. All transactions will be written to a permanent, unalterable audit log, which will include type of transaction, date/time, and user.

Developers and contractors will not have access to production PAM payment data.

Managers (other than PAM end users) will not have access to production PAM payment data. Procedures and responsibilities will be contained in user manuals and PAM Rules of Behavior.

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)

See #1 and #2 above

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 regulatory measures addressed?

Yes, Privacy Act clauses are in the contract.

Confidential Treatment of Federal Reserve System or U.S. Treasury Information.

All information and material related to (i) the security controls, and payment verification procedures of the Federal Reserve Banks and/or Federal Reserve System (collectively the "System"), and the United States Treasury and all related government agencies (ii) financial, statistical and personnel data pertaining to the Work, and (iii) financial, statistical, personnel, planning and similar information relating to past, present or future activities of the System or Treasury, (hereinafter collectively referred to as "Confidential Information"), which has or may come into the possession or knowledge of the Contractor, its agents or employees is confidential and proprietary information of the Treasury, Bank and/or the System. The Contractor shall, through written agreement, require its agents and employees not to disclose Confidential Information obtained while performing, or at the conclusion of, the Work to any person other than in connection with the performance of the Work. The Bank also considers the information contained in this RFP to be confidential information, which shall not be disclosed outside the Contractor's organization nor duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the RFP and prepare a response. The Contractor has no obligation of any kind with respect to any information which: (a) is already in the possession of the Contractor except that which has been received under another confidentiality agreement with the System or Treasury; (b) is rightfully received by the Contractor from a third party; (c) is independently developed by or for the Contractor; or (d) is or becomes publicly available.

The Contractor shall take all reasonable measures to enforce the agreements with its agents and employees required above. The Contractor shall take all reasonable measures mutually agreed to by the System and Contractor to recover any data or information wrongfully disclosed under the above provisions.

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

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

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

The FMS Business Owner (Assistant Commissioner, Regional Operations)

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, And Other)?

No

9) How will the data be used by the other agency?

Not applicable

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

The Chief Information Officer of FMS and the PAM Project Manager are responsible for proper use of the data.