



Financial Management Service

Privacy Impact Assessment

The Financial Management Service (FMS) Mission is to provide central payment services to Federal Program Agencies, operate the federal government's collections and deposit systems, provide government-wide accounting and reporting services, and manage the collection of delinquent debt owed to the government.

FMS Privacy Impact Assessments (PIA) <http://www.fms.treas.gov/pia.html>

Document Date: June 28, 2011

Document Version: 4.0

Name of System: RO Payments

SYSTEM GENERAL INFORMATION:

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

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. Within FMS, these responsibilities are assigned to the Assistant Commissioner for Payment Management (PM), under the control of the Chief Disbursing Officer (CDO). The CDO oversees the operations of four Regional Financial Centers (RFCs) that perform the actual payment creation.

The information in RO Payments relates to payments made on behalf of these FPAs to individuals and business entities. In order for the RFC to issue payments on behalf of an FPA, detailed information for the payment inscription is required from the agencies. This detailed information includes payee name, a payment amount, address/destination and a payment date.

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

N/A – RO Payments provides payment information to PACER On-Line which is the System of Record.

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

yes, explain.

no

N/A

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

yes

no

a. Is the information about members of the public? Yes, in that the system receives payment information from the Federal Program Agencies for individuals who are issued payments which includes members of the public.

b. Is the information about employees or contractors? No

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

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? None

b. What information will be collected from the public? None

c. What Federal agencies are providing data for use in the system? All FPAs for which FMS provides disbursing services (i.e., almost every Federal agency) will submit data to RO Payments

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 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. RO Payments 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?

FPAAs provide and certify the data received.

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

Input File Specifications and Outgoing 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 FPAAs 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?** N/A
- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain.)** N/A
- 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.)**
RO Payments 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, TIN, SSN or bank routing number.
- 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., 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?**

RO Payments 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?

With the exception of a subset of recurring 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.

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

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?

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 FMS 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?

Not Applicable

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?

Not Applicable

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

9) Access to the RO Payments 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 during the C&A 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. Certain roles have higher levels of access to the Privacy Act information and these roles have a signed Designation Letter detailing their specific responsibilities.

ACCESS TO DATA:

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

Check all that apply:

- Contractors
- Users
- Managers
- 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?

Some FMS users at Regional Financial Centers (RFC) can view payment data for all FPAs serviced by that RFC. 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 RO Payments System Security Plan.

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

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

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

Developers and contractors only have read access to production RO Payments data.

Managers (other than RO Payments end users) do not have access to production RO Payments data. Procedures and responsibilities will be contained in RO Payments 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)

Financial Management Service employees who serve as System Administrators have access to all payment data in RO Payments. RO Payments has a programmatically defined and controlled role for System Administrators (i.e., System Administrators are considered RO Payments users). All transactions are written to a permanent, unalterable audit log, which include type of transaction, date/time, and user.

System Operators do not have access to production RO Payments data.

Developers and contractors only have read access to production RO Payments payment data.

Managers (other than RO Payments end users) do not have access to production RO Payments data.

- 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 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?**

 yes

Xno

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?

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.

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

FMS Privacy Impact Assessments (PIA) <http://www.fms.treas.gov/pia.html>