Financial Management Service

Privacy Impact Assessment

PRInting and Check Enclosing (PRINCE)

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 24, 2011

Document Version: 2.0

Name of System: PRINting and Check Enclosing (PRINCE)

SYSTEM GENERAL INFORMATION:

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

PRINCE (PRINting and Check Enclosing) modernized the process of printing and enclosing checks, and check/letter mail pieces. PRINCE replaced the manual check wrapping equipment and legacy software sub-system with intelligent mail piece inserter equipment. PRINCE continues to print almost 200M check payments annually. PRINCE utilizes upgraded check processing software and hardware components, which provide improved accountability for each mail piece that is received from the payment systems. Check payment mail pieces are tracked through the check enclosing process until each mail piece is successfully enclosed for mailing. PRINCE streamlined the check processing and reduces the necessity for human intervention. PRINCE brings about improved internal controls and reduces the opportunity for human error and fraud. PRINCE was implemented in phases. Single channel and Dual channel KERN Inserting Sub-systems are operational at FMS' Regional Financial Centers (RFCs). Software sub-systems were developed to provide the accountability and tracking for enclosing checks, letters, and check/letter mail pieces. PRINCE also interfaces with FMS' Debt Management systems for offsetting payments and enclosing FedDebt letters . PRINCE may also include the implementation of the Automated Document Factory, which will provide further enhanced accountability for the processing of check mail pieces, track RFC load balances, and provide capabilities for rerouting check enclosing mail pieces to different Regional Finance Centers.

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

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

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

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 is received from the Regional Operations (RO) Payments System, Payment Automation Manager (PAM) , or the Debt Management System.

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 FMS and the Secretary of the Treasury the legal authority an authorization for the development of PRINCE.

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), the Secretary of the Treasury has the general authority to "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 Check, 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
   __ Third party

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

      PRINCE does not collect any information directly from taxpayers, employees, or other payees of Federal payments. All payment-related information is provided through the RO Payments, PAM, or Debt Management Systems from the Federal Program Agency (FPA) requesting the payments and/or collections to be made.

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

      PRINCE does not collect any information directly from the public. All payment-related information is provided through the RO Payments, PAM, or Debt Management Systems from the FPA requesting the payments and/or collections to be made.

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

      All FPA's that authorize and certify benefit, salary, vendor, and other payments to be disbursed by the Department of the Treasury.

   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?**

The various payment files described above are subject to automated validation processes prior to acceptance in order to assure accuracy. These validations ensure that information is properly formatted and meet validation rules as established by FMS and agreed upon by originating agencies.

Information related to the issuance and payment of check payments is also subject to validation by FMS in the normal course of reconciling and adjudicating check payments and supporting documents

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

Automated validation processes ensure that required fields and records in incoming data are filled according with rules established by FMS and agreed upon by originating agencies.

Authentication information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is complete.

Control totals follow NIST guidelines.

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

All payment file information provided by Treasury disbursed FPAs to the RO Payments or PAM systems goes through internal control and validation checks. The FPA separately certifies the payment data, item counts, and payment totals via the Secure Payment System (SPS). FMS then verifies that the control totals from these two separate processes match.

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

The data elements are described in the Input Files Specifications and Outgoing File Specifications that are contained in the Computer Program Specification Series (CPSS).

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?**

FMS is responsible for disbursement of US Treasury checks and FPA designated letters world-wide. The name and address that appear in the addressee space of mail-pieces (checks, letters and supporting documents) are required by the United States Postal Service for the proper delivery of payments or letters.

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?**

Not applicable. No individual records are kept.

4) **Can the system make determinations about employees or members of the 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?**

Not applicable.

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

Not applicable.

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.)**

Not applicable.

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?**

PRINCE does not collect any information directly from individuals.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

   Generally, there is a three to five day retention period of the payment data to allow for remakes of damaged checks, letters, and supporting documents. Disposition of the data at the end of the retention period is controlled by the system, returning the allocated space to the RISC AIX server operating system. Privacy information is not included in any PRINCE reports.

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

   Disposition of data at the end of the retention period is controlled by the system, returning the space to the RISC AIX server operating system. PRINCE does not maintain a system of record on check payments, and privacy information is not 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?**

   PRINCE applications and procedures are consistent at all sites. Application enhancements and problem changes are released through a Change Control Board process. Processing is monitored through the use of various logs, auditing and control systems.

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?**

   Auditing systems, both automated and manual, including access controls, are used to prevent unauthorized monitoring of individuals.

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**
   - **__ System Developers**
   - **__ Others (explain)_____**

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

   PRINCE users and administrators have access to the P5 550 AIX systems and the printed checks and mail piece items that are enclosed. This occurs in a controlled secured area that is restricted to only necessary personnel. Only employees who have a need to be in the area are allowed physical access to the area.

   System managers, contractors, and administrators have access to the data only in as much as they are responsible for the maintenance and upkeep of the system and structures in which the data is maintained and processed.

   Criteria and controls are contained in the PRINCE 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 the P5 550 AIX's data files in PRINCE. All transactions are written to a permanent, unalterable audit log which includes type of transaction, date/time, and user.

   Managers (other that PRINCE end users) do not have access to production PRINCE or RO Payment data. Procedures and responsibilities are contained in the PRINCE 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 #2 and #3 above. All FMS personnel must attend mandatory annual security and privacy training. This training includes a review of selected security and privacy procedures, regulations, and violation consequences. In addition, all personnel associated with the PRINCE system must sign a "Rules of Behavior" document. Those agreeing to the Rules of Behavior signify that they understand the information technology (IT)

security requirements, accept the IT security requirements, and acknowledge that disciplinary action may be taken based on violation of the Rules of Behavior. This applies to all FMS employees who access IT systems 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, Privacy Act clauses are included in the contract. The contractor is required to adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable to agency rules and regulations.

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

__yes
_X_no

No interfacing systems have access to data in PRINCE.

If yes,

a. Explain the interface.

Not applicable.

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

Not applicable.

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.

Not applicable.

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

Not applicable.

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