



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

Fiscal Service Privacy – Public Debt Impact Assessments
(PIA): http://www.treasurydirect.gov/privacy_impactassessment.htm

Document Date: June 21, 2011

Document Version: 1.0

Name of System: Secure Payment System

SYSTEM GENERAL INFORMATION:

1) System Overview:

The SPS application provides a mechanism by which government agencies can create payment schedules in a secure fashion. This application allows personnel at FPA locations to submit payment schedules to FMS using a browser and web interface. SPS also provides the regional financial centers a means to extract approved payment schedules for executing payment (e.g., check printing and electronic funds transfer). SPS is a "pass-through" system.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate?

The SPS system is not the system of record. However The SPS system is covered under a published System of Record Notices in the Federal Register.

.002 Payment Issue Records for 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

Payment data contains personal information subject to the Privacy Act, such as 1) payee name, 2) payee identifier e.g., Social Security Number, claim number, Taxpayer ID Number, 3) payee address (street address/post office box, or financial institution routing number and checking/savings account number), 4) payment amount. This data is submitted by the Federal Program Agency (FPA) requesting FMS to make the payment. The FPA has all data related to the payee (which can be an individual or a business entity). The FPA determines when payment is due, the amount of the payment, and the destination (address) of the payment. FMS has no role or responsibility in determining entitlement. FMS simply pays requests from FPAs which successfully pass FMS file formatting and balancing criteria and are properly certified by a designated agency certifying officer

a. Is the information about members of the public?

Yes

b. Is the information about employees or contractors?

Possibly, Yes.

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

Public Law (31 USC 3325) requires that "A disbursing official in the executive branch of the United States Government shall (1) disburse money only as provided by a voucher certified by (A) the head of the executive agency concerned; or (B) an officer or employee of the executive agency having written authorization from the head of the agency to certify vouchers." The SPS implements the requirements of this law. The functions (creation, certification, submission, and authentication/validation of payment schedules) supported by SPS are critical to the FMS payment business. SPS is the sole operational system available to provide agencies with the capability to create and submit electronic payment certifications to FMS, and for FMS to validate and authenticate the certifications prior to payment processing.

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?

SPS 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.

Payment data contains personal information subject to the Privacy Act, such as 1) payee name, 2) payee identifier e.g., Social Security Number, claim number, Taxpayer ID Number, 3) payee address (street address/post office box, or financial institution routing number and checking/savings account number), 4) payment amount. This data is submitted by the Federal Program Agency (FPA) requesting

FMS to make the payment. The FPA has all data related to the payee (which can be an individual or a business entity). The FPA determines when payment is due, the amount of the payment, and the destination (address) of the payment. FMS has no role or responsibility in determining entitlement. FMS simply pays requests from FPAs which successfully pass FMS file formatting and balancing criteria and are properly certified by a designated agency certifying officer.

b. What information will be collected from the public?

All payment-related information is provided by the Federal Program Agencies (FPAs) requesting the payment to be made.

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

All FPAs for which FMS provides disbursing services (i.e. almost every FPA) submits data through SPS.

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. FMS requires that the data be certified as proper for payment by a properly authorized FPA certifying officer. The certifying officer is responsible for the accuracy of the data beyond format and balancing.

b. How will data be checked for completeness?

Other than enforcing file format edits, FMS does not and cannot check the data for completeness. The certifying Officer checks data for accuracy.

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

Any data remaining in Main Database after 20 days will be deleted. Also see 3.a and 3.b above.

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

SPS User Manuals and SPS 440-Upload Format Document

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?**

Yes - SPS is a "pass-through" system necessary to make payments on behalf of agencies.

- 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?**

No

- 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.)**

N
/
A

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

N
/
A

- 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?**

N
/
A

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

SPS is not a reporting system. Other than permanent security audit files, SPS retains payment data for only 20 days after the payment is made. FPA users of SPS can view SPS data, but are restricted by automated controls within the application to only those payments certified by their own FPA.

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

Disposition:

Main Database - Payment schedules created by FPAs are deleted from Main Database upon extraction to the Mainframe. Any data remaining in Main Database after 20 days will be deleted.

Audit Database – Every time a record is inserted into the Main Database an audit record is created in the Audit Database. At this time SPS Audit records are kept indefinitely.

Archive Database – Every time a record is extracted to the Mainframe an archive record is created in the Archive Database. At this time SPS Archive records are kept indefinitely.

Extract Files (Certified Payment Schedules) sent to the RO Payment Mainframe.

Disposition of data is outside of SPS.

These procedures are documented in the SPS Security Plan and with the Records Management Branch.

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?

The SPS infrastructure is a distributed environment. The production data is signed and stored temporarily at the BPD site and disaster recovery site respectively. SPS utilized mirroring of the data between the production and DR sites.

4) Is the system using technologies in ways that FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes SPS is using technologies in a way that FMS has not previously employed. SPS uses public key infrastructure (PKI) certificate, smart cards and/or iKeys

SPS has many security features designed into the application such as the following:

1. SPS requires every user to have an individual token containing a public key infrastructure (PKI) certificate. This certificate must be used for every SPS session (i.e., every time the user accesses SPS).
2. Every user must be enrolled by FMS personnel in a SPS user table prior to being granted access to SPS. Enrollment requires submission of a paper form from a pre-established agency or "Designating Official." Even with a PKI certificate, a potential user does not have SPS access until entered into the user table.
3. The critical SPS function of submitting a payment schedule to FMS has been divided between two user roles (Data Entry Operator (DEO) and Certifying Officer (CO)) to enforce separation of duties. DEOs have the sole authority and capability within SPS to create, modify/edit, and delete payment schedules. COs have the sole authority and capability within SPS to certify payment schedules. A payment schedule cannot be successfully completed and submitted to FMS for payment generation without both the DEO and CO properly performing their SPS roles.
4. SPS appends the digital signature (a digital signature is the output of a cryptographic process which uses the public key certificate) stored on the

user's token of the DEO who created/modified a schedule each time the file (schedule) is closed. If multiple DEOs sequentially participate in creating a schedule, each DEO's digital signature is appended to the portion of the schedule(s) he created or modified. The digital signatures are maintained permanently in the SPS audit log at FMS.

5. SPS appends the digital signature of the CO who certified the payment schedule. The digital signatures are maintained permanently in the SPS audit log at FMS.
6. SPS maintains a permanent audit log record of every significant transaction in SPS. Among other details, the audit entry includes the identity of the user whose User Identification (userID) was logged on at the time the transaction occurred.
7. SPS protects the privacy and confidentiality of data in transit between the SPS client workstation or PC and the host SPS server via data encryption.
8. SPS employs "signed" software code to preclude running of unofficial or modified code, which could be used to illicitly modify, delete, or insert payments.
9. SPS sessions time out after a specified time period of inactivity at the user's workstation.

5) How does the use of this technology affect employee or public privacy?

System design and PKI encrypted data and digital signatures, protects the privacy and confidentiality of data.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes - End-user PKI credentials are issued by Data Access Control Division (DACD), which has a formal process as identified by the Fiscal Service PKI CP/CPS for credential issuance at different policies and assurance levels. Every record in SPS is digitally signed with a PKI credential. This digital signature, by law, ties that credential to the data and the creator of the data. An Audit record is created every time a record is inserted into the Main Database and an Archive record is created in the Archive Database every time a record is extracted to the Mainframe. This provides auditing information on who created the record, when the record was created, and what function was performed, including dollar amounts and can be tracked back to the source.

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

SPS has built in auditing capabilities that captures who, what, and when an action takes place.

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

The Bureau of the Public Debt and FMS has intrusion detection mechanisms on the SPS production and disaster recovery platforms which meet legally mandated guidelines. The SPS Rules of Behavior are presented to the users annually as part of an automated process built into the SPS application. User that do not read and sign the Rules of Behavior are automatically denied access into the SPS application. The Rule of Behavior are required as part of the IT security process (Section 4.1.2 of TD P85-01). . FPA users of SPS can view SPS data, but are restricted by automated controls within the application to only those payments certified by their own FPA.

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) DBA and Auditor Role

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

Each end user will be programmatically restricted to view and process data only for his/her own agency (actually, at the Agency Location Code (ALC) level). Access is strictly on a need to know basis. All users at a given FPA can view all payment data for that FPA. Only Data Entry Operators can create, modify, or delete payment data. 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 SPS requirements and architecture/design/development documentation. Procedures and responsibilities are contained in user manuals and SPS Rules of Behavior.

3) Will users have access to all data on the system or will the user's access be restricted? No Explain.

User access is restricted and have access only on a need-to-know basis.

User access is restricted to:

- Data Entry Operator (DEO) can only created, modify, delete its data for that FPA
- Certifying Officer (CO) can only view and certify data within it's FPA.
- RFCADMIN can only view users within it's RFC.
- SPSADMIN manages accounts for all RFC/FPA.

AUDITOR can view audit history of all SPS users.

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. In addition, all legitimate users must access SPS using a PKI certificate. All SPS users must be added to SPS user tables by a System Administrator. Without both a PKI certificate and existence on SPS user tables, browsing is prohibited. As explained previously, FPAs are responsible for determining all entitlement to payments they certify. Therefore, SPS grants all users from a given FPA (ALC) access to data for that ALC. Procedures and responsibilities are contained in user manuals and SPS Rules of Behavior. SPS is a role based system that restricts unauthorized browsing.

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 clause inserted in Section 17 of the Performance Work Statement, Order#: TFMS-HQ-09-K-0001

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

yes
 no

If yes,

a. Explain the interface.

SPS is an input into the PAM system.

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

The Information Owner and System/Business owner is responsible for the protection of privacy rights information. Once the data has been passed to PAM it is PAM's responsibility to protect the privacy rights of it's data.

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.**