Financial Management Service
Privacy Impact Assessment

Name of System/Application: Secure Payment System (SPS)

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

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. 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 Certification & Accreditation 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 Certification & Accreditation process, but is not required to be submitted with the OMB Exhibit 300 documentation).

NO

[1]

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

The SPS application provides a mechanism by which government agencies can create and certify payment schedules in a secure fashion.

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

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."

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system, e.g. employees, contractors, and taxpayers[2]?

The SPS enables Federal Program Agencies to create and authorize the movement of extremely large sums of Federal funds very quickly.

SPS has six types of user roles:

USER ROLES	DESCRIPTION
DEO	**Data Entry Operators** at agency locations to securely create and modify payment schedules
CO	**Certifying Officers** at agency locations to securely vet and certify payment schedules
OPER	**RFC Operators** to receive or extract certified schedules to host systems in order to execute payments
RFCADMIN	**RFC Administrators** allows RFC administrator to maintain system data and user access
SPSADMIN	**SPS Administrators** manage user and field validation tables.
AUDITOR	**Auditor** reviews audit log information and performs maintenance of audit data.

All SPS data is signed and encrypted. Neither the SPS Contractor’s nor FMS Employees have access to SPS production data.

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?**

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

b. **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.

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

   No State or Local Agencies are providing data to SPS.

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

   No third party source provides data to SPS.

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

   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.

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. **Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date?

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

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

Yes, data elements are described in the SPS.XSD located in the SPS documentation VOB of ClearCase .

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?**

N/A

4) **Can the system make determinations about employees/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?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

SPS payment data can be retrieved only at the aggregate schedule level. It cannot be retrieved within SPS by personal identifier. However, once a valid SPS user retrieves the aggregate data, (s)he can display the individual data.

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

N/A – SPS is not a reporting system.

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.)**

SPS does not interact between FPAs and individuals. All information collected is required to make the payment to the proper individual and assure its delivery to the proper address or account. Any additional information over and above that absolutely necessary to make the payment is at the discretion of the FPA and covered by FPA guidelines and regulations. Any declination or consent to provide information is handled by the FPA before payment action is requested.

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?**

The SPS alternate site (DR Site) is a Mirrored Site that is fully redundant facilities with full, real-time database mirroring.

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

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:
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.

4) **Is the system using technologies in ways that the 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 public/employee privacy?

The use of 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 kinds of information are collected as a function of the monitoring of individuals?

As part of the auditing process:

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.

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.

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

http://www.treas.gov/foia/privacy/issuances/fmspa.html
.002 - Payment Issue Records for Regular Recurring Benefit Payments
.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.**

No, the basic payment function of SPS will remain the same.

E. ACCESS TO DATA:

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

Each end user will be programmatically restricted to view and process data only for his/her own agency (actually, at the Agency Location Code level).

System Administrators will of necessity have access to all payment data in SPS.

Database Administrators will of necessity have access to all payment data in SPS.

System Operators will not have access to production SPS payment data.

Developers will not have access to production SPS payment data.

Managers (other than SPS end users) will not have access to production SPS payment data.

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? Explain.**

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.

See #1 and 2 above. Users have access only on a need-to-know basis.

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. 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.

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 clause inserted in Section 17 of the Performance Work Statement, Order#: TFMS-HQ-04-K-0012

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

Yes - The SPS application has a real-time interface to the FMS-DMS TOP database to determine if payees of SPS Same Day Payment requests have active delinquent debts. If the tax identification number (TIN) on the payment matches a TIN with an active delinquent debt, the creation of a Same Day Payment will be challenged by the SPS.

7) **Who will be 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.

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

Only FPAs submit data to SPS. Each FPA has access to its own data. No International, State, Local, or Other agency shares data or has access to it.

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

FPAs submit payment request data. FMS issues payments for validated requests.

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

The FMS Chief Information Officer, who directs the FMS IT security program/policies/standards, in conjunction with the business owner (the Chief Disbursing Officer of the United States), is responsible assuring proper use of all SPS.