The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (FS) 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 Impact Assessments (PIA):
https://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Secure Payment System

Document Version: 1.1

Document Date: 2-29-2018
Revised Date: 5-3-2018

SYSTEM GENERAL INFORMATION:

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

   Secure Payment System (SPS) is the access point to systems that provide centralized disbursement services to Federal agencies. SPS allows Treasury to issue payments on behalf of a Federal agency by providing a valid "certification" from the requesting agency. SPS is a highly secure method for the requesting agency to produce the legal authorization for the FS to make payments on its behalf.

   The SPS application provides a mechanism by which government agencies can create and certify payment schedules in a secure fashion. This application allows personnel at Federal Program Agencies (FPAs) locations to submit payment schedules to the Fiscal Service using a browser and web interface. FPAs input payment schedules in SPS and use information from SPS to verify that their schedules have been processed. Agencies can only verify that the information was sent to PAM. Certified payment schedules are streamed to Payment Automation Manager (PAM) for processing.

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

   FMS .002 Payment Records.

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.

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." 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 Fiscal Service payment business. SPS is the sole operational system available to provide agencies with the capability to create and submit electronic payment certifications to Fiscal Service, and for Fiscal Service 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:
X Employees
_ Contractors
_ Taxpayers
_ Others (describe)

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?**

Not Applicable.

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

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

Not Applicable.

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

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

All FPAs for which Fiscal Service 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?

Not Applicable.

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

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

Not Applicable.

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

3) Accuracy, Timeliness, and Reliability

a. How are data collected from sources, other than Fiscal Service records, verified for accuracy?

Payment data is entered into SPS by the Federal Program Agencies (FPA). Each FPA is responsible for the accuracy of the payment data submitted. SPS maintains no files as to the entitlement for any recipient of a payment that SPS issues at the request of an FPA. SPS requires that payment data is certified as proper for payment by an authorized FPA Certifying Officer (CO). The certifying officer is responsible for the accuracy of the data beyond format and balancing.

b. How will data be checked for completeness?

SPS enforces file format edits. SPS does not and cannot check the data for completeness. The Certifying Officer is responsible for checking data for accuracy and completeness.

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

Once the schedule has been properly certified by the Certifying Officer, the payment is streamed directly to the PAM system for processing. The schedule information remains in the SPS main database for 22 days for audit and archiving purposes. After 22 days the data is purged. Payment data is entered into SPS by the Federal Program Agencies (FPA). Each FPA is responsible for the accuracy of the payment data submitted. SPS maintains no files as to the entitlement for any recipient of a payment that SPS issues at the request of an FPA. SPS requires that payment data is certified as proper for payment by an authorized FPA Certifying Officer (CO). The certifying officer is responsible for the accuracy of the data beyond format and balancing. SPS enforces file format edits. SPS does not and cannot check the data for completeness. The Certifying Officer is responsible for checking data for accuracy and completeness.

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

The SPS data elements are described in the 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?**

   The SPS insures that the payment schedules are properly certified in order to make payments on behalf of FPAs.

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?**

   Not Applicable.

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

   The Certifying Officer is responsible of verifying schedule data.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   The database is protected by Fiscal Service firewalls. The SPS data is digitally signed and encrypted. Each end user will be programmatically restricted to view and process data only for his/her own Agency Location Code (ALC). Access is strictly on a need to know basis. Access is restricted by role. 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 (FPA Specific). Only a Certifying Officer (FPA Specific) can approve a payment for processing. Through separartion of duties it would take both the DEO and CO to create a proper payment. Fiscal Service users at Regional Financial Centers (RFC) can view only payment data for all FPAs serviced by that RFC. All SPS users must have an entry in the SPS user table and a valid PKI token to prevent unauthorized access.

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

   If processes are consolidated the databases are still protected by Fiscal Service firewalls. The SPS data is digitally signed and encrypted. Each end user will be programmatically

restricted to view and process data only for his/her own Agency Location Code (ALC). Access is strictly on a need to know basis. Access is restricted by role. 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 (FPA Specific). Only a Certifying Officer (FPA Specific) can approve a payment for processing. Through separartion of duties it would take both the DEO and CO to create a proper payment. Fiscal Service users at Regional Financial Centers (RFC) can view only payment data for all FPAs serviced by that RFC. All SPS users must have an entry in the SPS user table and a valid PKI token to prevent unauthorized access.

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.)**

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, The SPS user can display the individual data.

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

SPS is not a reporting system. However, Auditing reports can only be accessed through the AUDITOR role. the Audit Report is used for after the fact investigation of possible incidents. It can track activity in SPS of who, what, and when, and the signed Rules of Behavior (ROB) report is used to validate user that have read, signed, and fully understand the security requirements.

10) **What opportunities do individuals have to decline to provide information (i.e., in such cases 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?**

Not Applicatble.

Payment data comes only from an FPA.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

The Bureau of the Fiscal Service and Reporting records are retained for 6 years 3 months. Accountable Officer Accounts records are retained IAW GRS 6, Items 5, 10 and GRS 1.1. Item 011, 020 PKI Administrative records are retained for 7 year 10 year or 20 years GRS 3.2. Item 060 PKI Administrative records are retained in accordance with N1-GRS-07-03 records can be retained for 7 year 10 year or 20 years based upon the highest level of operation of the CA or whenever no longer needed for business needs, or whichever is greater.

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

Excluded are all copies (paper and electronic) of Tribal Trust Litigation payment records which are currently under a records legal hold and must be preserved indefinitely until case is settled.

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?

SPS only operates at one site at a time. The alternate production site is a mirrored site identical to the primary site. The data is maintained at both sites simultaneously using data mirroring.

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

Yes.

SPS is using technologies in a way that Fiscal Service 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:

- 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).

- Every user must be enrolled by Fiscal Service personnel in a SPS user table prior to being granted access to SPS. Enrollment requires submission of a paper form from a preestablished agency or "Designating Official". SPS users must have both a valid PKI certificate and entered into the SPS User table to be a valid SPS user.

- The critical SPS function of submitting a payment schedule to Fiscal Service 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 Fiscal Service for payment generation without both the DEO and CO properly performing their SPS roles.

- 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 Fiscal Service.

- 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 Fiscal Service.

- 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.

- All SPS data is encrypted in transit and at rest.

- SPS employs "signed" software code to preclude running of unofficial or modified code, which could be used to illicitly modify, delete, or insert payments.

- 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?**

   SPS uses Public Key Infrastructure to protect the privacy and confidentiality of its data through the use of encryption and digital signatures**.**

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

   Yes.

   SPS has a built in audit function. This gives the AUDITOR role within SPS the ability to track 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. However it does not have the ability to track location.

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

   SPS the ability to track who created the record, when the record was created, and what functions were performed, including dollar amounts and can be tracked back to the source.

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

   The Auditing function is restricted to the AUDITOR role in SPS.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   - **__ Contractors**
   - **X 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?**

User access is restricted to need-to-know basis and by user roles.

Data Entry Operator (DEO) - can only create, modify, delete its data for that FPA.
Certifying Officer (CO) - can only view and certify data within its FPA.
RFCADMIN - can only view users within its RFC.
SPSADMIN - manages accounts (cannot alter data) for all RFC/FPA.
AUDITOR - can view audit history of all SPS users.

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

User access is restricted to need-to-know basis and by user roles.

Data Entry Operator (DEO) - can only create, modify, delete its data for that FPA.
Certifying Officer (CO) - can only view and certify data within its FPA.
RFCADMIN - can only view users within its RFC.
SPSADMIN - manages accounts (cannot alter data) 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)**

Each end user will be programmatically restricted to view and process data only for his/her own Agency Location Code (ALC). Access is strictly to 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. Fiscal Service 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, architecture, design, and development documentation. Procedures and responsibilities are contained in user manuals and SPS Rules of Behavior.

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.

Contract# GS-35F-4775G, Order# TFSAFSA14K0028, Attachment B, List of Security Requirements The Contractor shall comply with both Fiscal Service and Treasury requirements that extend above federal government and industry information technology regulatory requirements and standards. The Contractor's performance and systems shall comply with the most current versions of the following applicable Federal and industry

information technology regulatory requirements and standards. "The Privacy Act of 1974, as amended, 5 U.S.C. § 552a http://www.usdoj.gov/oip/privstat.htm.".

6) **Do other systems share data or have access to the data in the system?**
   X **yes**
   _ **no**

   If yes,

   a. Explain the interface.

   All interfacing systems are internal Bureau of the Fiscal Service systems.

   SPS interfacing systems:

   - Payment Automation Manager (PAM) whereby SPS streams agency schedule certifications to PAM and PAM acknowledges receipt.
   - Debt Management Service's Treasury Offset Program (TOP) uses SPS data to identify Fiscal Service eligible payments.
   - Government Wide Accounting's (GWA) Shared Accounting Module (SAM) provides SPS the ALC and TAS-BETC file to validate payment request.

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

   The Business owner is responsible for the protection of privacy rights information. Once the data has been passed to the interfacing systems it is the responsibility of that system to protect the privacy rights of its data.

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.

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