Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 426
System Name: SmartPay - Data Warehouse
CPO Approval Date: 3/29/2023
PIA Expiration Date: 3/28/2026

Information System Security Manager (ISSM) Approval

Jonathan Wallick

System Owner/Program Manager Approval

Narendra Rao Namana Mohanakrishna

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
SmartPay - Data Warehouse

B: System, application, or project includes information about:
Federal Employees and contractors have their information retained.

C: For the categories listed above, how many records are there for each?
12 Million Unique Charge Card Accounts as of 03/16/2023

D: System, application, or project includes these data elements:
SmartPay 2: (Nov 2018, contract ended)

SmartPay 2 data contract ended in Nov 2018 but SPDW still maintains SmartPay 2 data as part of the data retention policy which contains:

— Account Number — Social Security Number — Addendum Key — Purch ID — Transaction Unique Key — Cardholder Unique ID — Street Address — Cardholder Work Phone Numbers — Cardholder Fax Phone Numbers — Cardholder Email Address Text — Short Card Numbers — Merchant Identifier — First and Last Names

SmartPay 3:

Do not contain any personal information including PCI and PII.

Overview:

SmartPay Data Warehouse is a GSA Federal Acquisition Services (FAS) Major Information System (MIS). SmartPay Data Warehouse serves as a repository for data provided by various banks supporting the GSA charge card program. SPDW holds data that can be used to view transaction information, dispute transactions, and create reports. This information is viewable by authorized users within SmartPay Data Warehouse Cloud Minor Application.
SmartPay Data Warehouse provides a program wide view of government charge card data. The major requirements that GSA SmartPay Data Warehouse accomplishes with the Data Warehouse are as follows:

- Spend Analysis – Analyzing spend to identify patterns and support strategic sourcing initiatives focused on leveraging volume buys to negotiate merchant discounts and achieve other procurement savings;
- Risk Identification – The use of "rule based" methods and other data mining capabilities to identify high risk transactions, minimize the potential for, and detect incidences of misuse, fraud, waste, and abuse;
- Performance Measurement and Reporting – The use of performance metrics and reporting to improve overall card program management;
- Refund Management and Compliance Monitoring – The use of data and data management tools to improve the receipt of refunds and monitor banks' adherence to refund and fee/pricing commitments;
- Tax Reclamation: Analyzing transaction data to identify and assist with the recovery of State and Local taxes that have been inappropriately assessed on Federal government charge card transactions.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Any other legal authority can be found in the SmartPay Master Contract, which can be granted access upon request.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
No

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?

1.2b: Explain why a SORN is not required.
Information is not searchable by a PII. PII/PCI data sent by the banks remains encrypted in flat files on eagu1p. The only data that is searchable would be the Charge Card numbers within the database, but there is no PII in reference to those card numbers.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
C.7.2.4 of the SmartPay Master Contract specifies the retention period for all materials relating to SmartPay Data Warehouse. Utilized within the contract is: FAR 4.805 Storage, handling, and contract files and NARA General Records Schedule 01.1/010 (DAA-GRS-2013.0003.0001). SPDW utilizes the FAR definition of "final contract payment" rather than using the "occurrence of each transaction" as its counting commencement date. Note: year within the contract is in reference to fiscal years. Within SPDW, "standalone" PII that is maintained to fill future transactions is included under: PII Record Extracts and Logs (for reports, upgrades, migration purposes) - Record Title: Personally Identifiable Information Extracts - OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify". This data is Temporary. It is to be destroyed when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate per: DAA-GRS-2013-0007-0012 (GRS 04.2/130). Additionally, Personally Identifiable Information Extract Logs should be maintained for a temporary period of time and destroyed when business use ceases.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
As a part of SmartPay 2 contract, banks send flat files containing the required information (Charge card numbers, and transaction data), but additionally within those files, PII is contained. That PII data is not required and left encrypted on Eagu1P as a result. PCI Data is collected in order to aggregate and track federal spending.

SmartPay 3 is no collecting any PII or PCI information.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
As a part of SmartPay 2 contract, there are multiple protections in place in order to protect the data. Column level encryption protects the charge card numbers within the database, and in addition there is disk level encryption for the database. The processing server where the remainder of the PII/PCI is retained maintains disk level encryption and the files themselves are GPG encrypted. Beyond that, the charge card numbers are aggregated and can not be viewed in reports or dashboards. Lastly, the datacenters where the servers reside are T3 datacenters with a host of physical and digital controls.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.

3.5 What kinds of report(s) can be produced on individuals?
No reports are created for individuals, reports CAN be created for a specific charge card number, but that CC is not tied to an individual in the Database.

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
Not applicable, no reports or dashboards contain individual's information.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
No

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
None

4.2How: If so, how will GSA share the information?
Data is shared through two online portals, one of which is only accessible by internal GSA users, and the other by the public and other federal agencies. Without authentication, a very limited section of the data is viewable. This publicly viewable data is Spend, Purchase, Travel, Refund, and Fleet data collected through the program. All data viewable through the portals is aggregated and contains no personally identifiable information or PCI data.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
Information is gathered by banks and sent by banks to the GSA.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

4.4WhoHow: If so, who and how?
The internal interaction is the transfer of data files containing no charge card numbers and no PII data to TAMS on the ClearPath infrastructure over port 22. Unisys will reach out in the event of a security incident. Data is accepted in GPG encrypted flat file format from banks over port 22 using the SFTP protocol. There is a formal agreement between SPDW and SmartPay Bank Contract Holders (CitiBank & USBank) which spell out conditions for incident reporting.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
No standards are followed for data quality " GSA follows nonspecific standards, namely (ISO-8000 & ISO 22745). All flat files at rest remain GPG encrypted (RSA 2048). GPG Encryption is done by the Red Hat Enterprise Linux libgcrypt Cryptographic Module (cert# 2657), Chargecard Numbers pulled from the files are stored in the SmartPay Data Warehouse database which maintains disk encryption in addition to the column-level data key encryption (Column level provided by OpenSSL, cert# 2473).

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Back end developers, System Admins, internal and external non-privileged users.

6.1b: What is the authorization process to gain access?
A back end developer and System Admin will log into their GFE using their PIV card. They will create an SSH session into a JumpBox using their developer accounts credentials. Developer accounts are a separate account from the ENT maintained in Active Directory. From the Jumpbox they can then SSH into the servers that their developer account is privileged to. Privileges to servers and permission within said server, are all maintained within the UNIX groups. There are two types of non-privileged users, internal and external. If a non-privileged user is internal to the network, the user will navigate to either the SmartPay Portal URL or FCS Tableau server through their web browser of choice, where SecureAuth SSO will then authenticate them. If the user is external to the network, they must sign into the SmartPay Portal which will require an account (created by help desk). OKTA will then challenge them for their OTP before entry. All permissions and accounts are maintained through Active Directory or OKTA.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
9/7/2024

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The Stennis environment that houses the SPDW system has technical and physical security protections required for a FISMA Moderate system. The environment technical and physical and controls are detailed in the SPDW SSPP. The SPDW FISMA system has Technical controls that are documented in the SPDW SSPP: - Identification and Authentication - Access Controls - Event auditing - Encryption at rest and transport - Vulnerability Scanning and Remediation The SPDW FISMA system has Managerial controls that are documented in the SPDW SSPP and on the SPDW Google Team Drive as well as Service Now: - Security Training - User access request procedures - Annual user recertification - Key management procedures - Audit Review, Analysis, and Reporting - Security Assessments - Incident Reporting and Incident Response Plan

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
An IRP has been created to respond to suspected or confirmed security incidents. It can be found within the the SPDW Google Drive. The IRP has not been tested, but it will be undergoing a table top during the annual DR testing.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Individuals do not have any opportunities to consent or decline to provide information to the SmartPay Data Warehouse.

7.1Opt: Can they opt-in or opt-out?

No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
Their only ability to opt out would be to not receive a charge card. SmartPay Data Warehouse does not collect any information, it only acts as a repository of information for the SmartPay Charge Card Program.

7.2: What are the procedures that allow individuals to access their information?
There is no currently defined process for an individual to access their information within the SmartPay Data Warehouse. In theory, The Privacy Act or FOIA would allow a user to request their spending data, but only specifically their data. This would be an ad-hoc and manual process to retrieve that individual's access.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
All GSA staff and contractors are required to take the mandatory annual Privacy training. GSA IT produces a report to identify individuals who have not taken the training and ensure the training is completed by everyone.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
The System Owner validates that EIO will audit Database and OS logs for the SmartPay Data Warehouse as part of the Enterprise Logging Program. The System Owner also ensures that controls in the SSPP are validated by a third party who will audit the technical and policy safeguards, which conjoined with the PIA ensuring that information is used appropriately.