SmartPay Data Warehouse

Privacy Impact Assessment (PIA)

June 12, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Jonathan Wallick

Name of Program Manager/System Owner:

- Narendra Rao

Signature Page

Signed:

DocuSigned by:
Jonathan Wallick
51A2B47547C34D9...

Information System Security Manager (ISSM)

DocuSigned by:
Narendra Rao
776FE828D4EF405...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0

Table of contents

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about *SmartPay Data Warehouse.* To accomplish its mission *GSA-IT* must, in the course of managing *SmartPay Data Warehouse* 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]

A. System, Application, or Project Name:

SmartPay Data Warehouse (SPDW)

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?

8 Million Unique Charge Card Accounts as of 2/7/2020

D. System, application, or project includes these data elements:

- 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

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 the various banks in support of the GSA charge card program. It holds data that can be used to view transaction information, dispute transactions, and create reports

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.

Securing Sensitive PII and PCI Data

Data is secured during transport via SFTP(22) and the files during transport retain their GPG (RSA 2048) encryption. All flat files at rest are GPG encrypted using RSA 2048 encryption. 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.

The EIO protects GSA data that resides (rests) on GSA's disk storage devices by securing the disk storage devices within secure Tier-3 data center facilities. These facilities are secured by multiple levels of protection; from locked and pass-key protected reinforced doors to 24x7 on-site authorized security guards. All forms of data media are protected by AES256 level encryption. Data is further protected by state-of-the-art closed circuit surveillance systems as well as early detection systems for smoke, fire, and water. Data residing on backup tapes is protected in two locations: duplicate backup tapes are stored in GSA secure tape libraries which are located within GSA secure data centers, and off-site tapes are stored at a GSA-authorized and secure off-site storage location: Iron Mountain.

Use of PII & PCI

SmartPay Data Warehouse only uses the charge card numbers, which are placed into the SmartPay DataWarehouse Database. The system which holds the PII and PCI is within a separate environment on a separate vlan. The database maintains disk encryption in addition to the column-level data key encryption using AES256 encryption. The remainder of the PII and PCI remains untouched and GPG encrypted on the processing server. It will be retained there for 7 years as per policy.

PII Sharing with GSA systems

Data files containing PII/PCI are sent over SFTP to the Transportation Audit Management System (TAMS) to support their business mission. Data is aggregated into a non PII/PCI format which is available to users on the SmartPay Portal and Business Objects dashboards.

SECTION 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? If so, what System of Records Notice(s) apply/applies to the information?

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)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

Not Applicable as this is not an information collection.

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

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.

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

As a part of the cardholder agreement, personal data is provided to the banks. Please see C.7.4.2.2 of the SmartPay Master Contract (covered in the system of records) for more information. SmartPay provides aggregated reporting that does not include individual user information. A specific individual's data sharing from the SmartPay Data Warehouse is limited to specific circumstances such as: Congressional requests, IG requests and investigations, or requests by other need to know organizations.

SECTION 3.0 DATA MINIMIZATION

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

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.

3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

Data about individual users is not used and simply retained in an encrypted format for the obligated seven (7) years.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

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’t 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?

The system does not monitor the public, GSA Employees, or contractors in any capacity.

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

Not applicable, no reports or dashboards contain individual's information.

SECTION 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 – in the flat files sent by the banks, there is a significant amount of PII & PCI data which is sent in addition to the information which is required for SmartPay Data Warehouse to function – however that data is left alone and encrypted on the processing server.

4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?

Yes. Data is shared with other federal agencies.

Agency Group	**Agency Name**
All Other Agencies	Legislative Branch
All Other Agencies	Federal Retirement Thrift Investment Board
All Other Agencies	Merit Systems Protection Board
All Other Agencies	Federal Maritime Commission
All Other Agencies	African Development Foundation

All Other Agencies	Inter-American Foundation
All Other Agencies	Peace Corps
All Other Agencies	Armed Forces Retirement Home
The Judicial Branch	The Judicial Branch
Executive Office of the President	Executive Office of the President
Department of Agriculture	Department of Agriculture
Department of Commerce	Department of Commerce
Department of Interior	Department of Interior
Department of Labor	Department of Labor
Department of Defense	Department of the Navy
Department of Defense	U.S. Marine Corps
Department of Defense	Department of the Army
Department of Defense	Department of the Air Force
U.S. Postal Service	U.S. Postal Service
Department of State	Department of State
Department of Treasury	Department of Treasury

Office of Personnel Management	Office of Personnel Management
National Credit Union Administration	National Credit Union Administration
Social Security Administration	Social Security Administration
Nuclear Regulatory Commission	Nuclear Regulatory Commission
Smithsonian Institution	Smithsonian Institution
Smithsonian Institution	National Gallery of Art
Department of Veterans Affairs	Department of Veterans Affairs
General Services Administration	General Services Administration
National Science Foundation	National Science Foundation
Federal Deposit Insurance Corporation	Federal Deposit Insurance Corporation
Federal Labor Relations Authority	Federal Labor Relations Authority
Department of Defense - Independent Agencies	Department of Defense - Independent Agencies
Consumer Product Safety Commission	Consumer Product Safety Commission
Environmental Protection Agency	Environmental Protection Agency
Department of Transportation	Department of Transportation

Department of Homeland Security	Department of Homeland Security
Overseas Private Investment Corporation	Overseas Private Investment Corporation
Agency for International Development	Agency for International Development
Small Business Administration	Small Business Administration
Department of Health and Human Services	Department of Health and Human Services
Farm Credit Administration	Farm Credit Administration
National Aeronautics and Space Administration	National Aeronautics and Space Administration
Export Import Bank	Export Import Bank
Department of Housing and Urban Development	Department of Housing and Urban Development
National Archives and Records Administration	National Archives and Records Administration
Department of Energy	Department of Energy
Department of Education	Department of Education
U.S. Senate	U.S. Senate
Government Accountability Office	Government Accountability Office

Appalachian Regional Commission	Appalachian Regional Commission
Department of Justice	Offices, Boards, and Divisions
Department of Justice	Drug Enforcement Administration
Department of Justice	Bureau of Prisoners
Department of Justice	U.S. Marshals Service
Department of Justice	Federal Bureau of Investigation
Department of Justice	Office of Justice Programs
Department of Justice	Bureau of Alcohol, Tobacco, Firearms and Explosives

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 publically 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 directly from the individual or is it taken from another source? If so, what is the other source(s)?

Information is gathered by banks and sent by banks to the GSA. The Information is supplied by other sources as the federal government is not a bank with charge cards.

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

There is interaction outside of the boundary within the GSA three times, and once outside of the GSA. The first interaction within the GSA, is the sharing of aggregated data between the

Business Objects environment and EAGU1Ps' Sybase IQ 16.4 Database over HTTPS(443) and SQL (2638). The second of the internal interactions is with the Unisys data center where the SmartPay Portal is hosted in the ClearPath environment. Aggregated data from the Sybase IQ 16.4 Database is shared over HTTPS (443) and SQL (2638) to the portal. The third internal interaction is the transfer of data files containing charge card numbers and non-pii data to TARPS (to become TAMS) on the ClearPath infrastructure over port 22. Clearpaths' environment has undergone a security Assessment and Authorization. Unisys will reach out in the event of a security incident. Lastly, 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.

SECTION 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 – note latest operating environment tested was 7.4), 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).

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the system, application, or project? 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 Business Objects URL 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. This authentication process is described further in 10.4. All permissions and accounts are maintained through Active Directory, including non-internal users who have a separate AD domain.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes – extension granted 1/23/2020

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 SSP.

The SPDW FISMA system has Technical controls that are documented in the SPDW SSP:

- 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 SSP and on the SPDW Google Team Drive as well as Service Now:

- Security Training
- User access request procedures
- Annual user recertifications
- 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? If so, 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.

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Individuals do not have any opportunities to consent or decline to provide information to the SmartPay Data Warehouse. 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 procedures 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? If so, how?

Users can not amend information to themselves via SmartPay directly as the SmartPay Data Warehouse simply acts as a repository. All information is collected by banks and sent to the SmartPay Data Warehouse post data collection. Any requests to amend or remediate information would need to be through the users bank.

SECTION 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.

SECTION 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 SSP are validated by a third party who will audit the technical and policy safeguards, which conjoined with the PIA ensure that information is used appropriately.

---

[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.