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: 441
System Name: GSA SmartPay Content Systems (GSPCS)
CPO Approval Date: 8/4/2023
PIA Expiration Date: 8/3/2026

Information System Security Manager (ISSM) Approval

Arpan Patel

System Owner/Program Manager Approval

David Shea

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
GSA SmartPay Content Systems (GSPCS)

B: System, application, or project includes information about:
GSPCS is a Major Information System comprising two public internet web sites – smartpay.gsa.gov and training.smartpay.gsa.gov hosted on the Cloud.gov platform. The Cloud.gov platform-as-a-service provides a hosting

environment and brokered PostgreSQL database and Redis services used by the GSA SmartPay training website. GSPCS also hosts the Section 889 Tool.

The purpose of smartpay.gsa.gov site is to distribute GSA SmartPay information to customer agencies. The site specifically covers the GSA SmartPay program overview, eligibility, program statistics, new legislation, logo and design, tax information, policies, glossary, and other resources. All content available on the smartpay.gsa.gov site is approved for public release by GSA.

GSA Smartpay also offers web-based training offered through training.smarpay.gsa.gov website. This is a free, online training resource offered for the proper use management of the GSA Smartpay purchase card and travel card program for customer agencies. The site includes training courses for GSA SmartPay cardholders and program coordinators which helps customer organizations comply with OMB Circular A-123, Appendix B, “A Risk Management Framework for Government Charge Card Programs” requirements.

The GSA SmartPay, training websites, and the 889 Tool do not offer any login functionality for non-privileged users. Privileged users can login to the application using GSA SecureAuth with MFA. Members of the public will be able to view the contents for the GSA Smartpay program. The main GSA SmartPay website is a static website intended for public users.

The GSA SmartPay site and 889 Tool do not collect user information. The GSA SmartPay training site collects personal information that is limited to only names and e-mail addresses for training record purposes. While it is advised to use business e-mail addresses, users can provide personal e-mail addresses at their own discretion to provide flexibility for those users that do not have business email addresses. The impact levels are considered low given the minor harm that may be caused to those individuals and GSA if the personal email addresses are disclosed, altered, or unavailable.

Web-based training offered through training.smarpay.gsa.gov website is a free, online training resource offered to GSA Smartpay purchase cardholders. The site provides training courses for GSA SmartPay cardholders and program coordinators which helps customer organizations comply with OMB Circular A-123, Appendix B, “A Risk Management Framework for Government Charge Card Programs” requirements.

The Cloud.gov Pages service that generates the front-facing static website requires two-factor login by the developers and all users are GSA employees or contractors. The GSA SmartPay static website is for public consumption.

Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232) prohibits the purchase of covered telecommunications equipment and services from vendors who sell products containing spyware. These devices could pose a threat to U.S. security by spying on or disrupting communications within the U.S. In addition, contractors are required by the Federal Acquisition Regulation (FAR) to provide information on whether or not they are supplying covered telecommunications under contracts and orders with the Federal Government. This prohibition became effective August 13, 2020 and applies to all contracts, regardless of dollar amount, including micropurchases on charge cards, as well as formal contracting actions.

The Section 889 Tool allows GSA SmartPay stakeholders to determine if a vendor is registered in the System for Award Management (SAM), if they have completed the representations required by the FAR 52.204-26 provision, and what responses were provided. The tool uses an application programming interface that provides stakeholders (who would not normally access SAM) with a streamlined way to check the SAM.gov website for the entity’s 889 representations summary information.

C: For the categories listed above, how many records are there for each?
This includes accounts that have been accessed within the last 7 years, in accordance with NARA archiving requirements. This reflects current usage of our existing websites (to be decommissioned once our new websites are deployed on cloud.gov)

D: System, application, or project includes these data elements:
For the training website, emails include federal government entity emails (e.g., .gov, .mil) and a small subset of non-government email domains (e.g., .org, .edu, .net, .com). Note that these non-government emails may include those used for personal use.

The 889 Tool is a simple search tool that pulls vendor's 889 compliant data from SAM.gov via a public API key. The 889 tool does not store any type of data.

Personal email addresses collected and stored in our training website are considered PII. Based on the 7/24/23 discussion with GSA CSIO and GSA Privacy Office Representative we updated the FIPS 199 and SSPP to reflect a low impact system category. We also provided the below justification for downgrading the impact level from Moderate to Low.

C.2.8.9 Personal Identity and Authentication Information

Confidentiality: This level was downgraded from Moderate to Low because only personal email addresses can be disclosed. No other PII is collected. Users are encouraged to use business email addresses when registering for training on the site. A banner is presented to the user during registration advising the user to use a business email address and informing the user of the usage of their email address and associated risks. There is only a small subset of users that use personal email addresses over business email addresses since they do not have a business email address. This includes users like tribal agency personnel. If a person's personal email address is disclosed this poses minor harm to the individuals and to the agency as the risk is insignificant. The personnel email address is encrypted in transit (using TLS v1.2) and at rest (using AES 256).

Integrity: This level was downgraded from Moderate to Low because there is minor harm if a person’s email address is altered. This is only needed to retrieve past certificates. A new email can be used or the person can contact the GSA SmartPay Program.

Availability: This level was downgraded from Moderate to Low because there is minor harm if a person’s personal email address is unavailable. This is only needed to retrieve past certificates. A new email can be used or the person can contact the GSA SmartPay Program.

Overview:

GSPCS is a Major Information System comprising two public internet web sites – smartpay.gsa.gov and training.smartpay.gsa.gov hosted on the Cloud.gov platform. The Cloud.gov platform-as-a-service provides a hosting environment and brokered PostgreSQL database and Redis services used by the GSA SmartPay training website. GSPCS also hosts the Section 889 Tool.

The purpose of smartpay.gsa.gov site is to distribute GSA SmartPay information to customer agencies. The site specifically covers the GSA SmartPay program overview, eligibility, program statistics, new legislation, logo and design, tax information, policies, glossary, and other resources. All content available on the smartpay.gsa.gov site is approved for public release by GSA.

GSA Smartpay also offers web-based training offered through training.smarpay.gsa.gov website. This is a free, online training resource offered for the proper use management of the GSA Smartpay purchase card and travel card program for customer agencies. The site includes training courses for GSA SmartPay cardholders and program coordinators which helps customer organizations comply with OMB Circular A-123, Appendix B, “A Risk Management Framework for Government Charge Card Programs” requirements.

The GSA SmartPay, training websites, and the 889 Tool do not offer any login functionality for non-privileged users. Privileged users can login to the application using GSA SecureAuth with MFA. Members of the public will be able to view the contents for the GSA Smartpay program. The main GSA SmartPay website is a static website intended for public users.

The GSA SmartPay site and 889 Tool do not collect user information. The GSA SmartPay training site collects personal information that is limited to only names and e-mail addresses for training record purposes. While it is advised to use business e-mail addresses, users can provide personal e-mail addresses at their own discretion to provide flexibility for those users that do not have business email addresses. The impact levels are considered low given the minor harm that may be caused to those individuals and GSA if the personal email addresses are disclosed, altered, or unavailable.

Web-based training offered through training.smarpay.gsa.gov website is a free, online training resource offered to GSA Smartpay purchase cardholders. The site provides training courses for GSA SmartPay cardholders and program coordinators which helps customer organizations comply with OMB Circular A-123, Appendix B, “A Risk Management Framework for Government Charge Card Programs” requirements.

The Cloud.gov Pages service that generates the front-facing static website requires two-factor login by the developers and all users are GSA employees or contractors. The GSA SmartPay static website is for public consumption.

Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232) prohibits the purchase of covered telecommunications equipment and services from vendors who sell products containing spyware. These devices could pose a threat to U.S. security by spying on or disrupting communications within the U.S. In addition, contractors are required by the Federal Acquisition Regulation (FAR) to provide information on whether or not they are supplying covered telecommunications under contracts and orders with the Federal Government. This prohibition became effective August 13, 2020 and applies to all contracts, regardless of dollar amount, including micropurchases on charge cards, as well as formal contracting actions.

The Section 889 Tool allows GSA SmartPay stakeholders to determine if a vendor is registered in the System for Award Management (SAM), if they have completed the representations required by the FAR 52.204-26 provision, and what responses were provided. The tool uses an application programming interface that provides stakeholders (who would not normally access SAM) with a streamlined way to check the SAM.gov website for the entity's 889 representations summary information.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
Our main website is consited of static pages which provides helpful GSA SmartPay information to cardholders. Our training website provides certain charge card account holders and manager training. Our 889 tool is a simple search tool that returns vendor's 889 compliant status. We do not require any legal authority to operate our current websites and 889 tool. We do not anticipate a need for any legal authority to deploy the new websites on cloud.gov. Migrating the 889 tool from the Google Cloud Platform (GCP) is a simple lift and move from GCP to cloud.gov.

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.

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.
We adhere to NARA's record retention requirements.

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.
Our training website will include the following banner:

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

We only obtain your information necessary to access this system. We collect information such as agency name and email address, to issue training certificates and for agency reporting management. We carefully protect your information and will not make it available to web tracking software for retention. We do not disclose, give, sell, or transfer any personal information about our visitors, unless required for law enforcement or statute.

To access the GSA SmartPay training system, please use your business or work email only, and not a personal email address

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
The way our training website works is the end user provides their email address and the system sends them a secure link where they can click on to receive the training. The same process works if the end user needs to take a quiz

upon completing their training. The system uses the end user's email address as a way to authenticate them. Email addresses are also used for Agency Official Program Coordinator (A/OPC) to pull reports on their cardholders' training data.

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?
We have encryption for data at rest and in-transit as specified in the SSPP.

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?
A/OPC can run reports on training completion for their agency's cardholders.

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?
The data will not be de-identified because the only PII we are storing is email addresses, of which a small subset is personal email addresses.
Employees from agencies such as DOD often cannot access websites outside of DOD firewall to take training. As such they often end up using their personal email addresses to take training on our training website.
Tribal organizations often use .net and .com email addresses to take training from our training website.

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?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Federal Agencies

4.2How: If so, how will GSA share the information?
We (GSA SmartPay) do not share training completion data. However, agency's A/OPC can pull training completion report for their agency's cardholders.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

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 889 tool pulls vendor's 889 compliant data from SAM.gov via the public API key.

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
We are in the process of working with SAM.gov to put an ISA 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?
Our training website collects: first name, last name, agency (and bureau if applicable), email address.
GSPCS does not store or process PII, PCI, or Business Sensitive data with the exception of personal email addresses (considered PII) that may be used for the training site for training record purposes only
Currently the system does not have the ability to verify the data for accuracy.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Developers, System Administrators, System Owner

6.1b: What is the authorization process to gain access?
We have the entire account management (AC-2) described in the SSPP. We also have this process as an artifact that we can share with the Privacy Office for review.

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.
9/29/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Our websites and 889 Tool will be deployed on cloud.gov. We will be inheriting many of the controls from cloud.gov. Cloud.gov is a FedRAMP certified platform; as such our system will be hosted at the application level on cloud.gov.
All database encryption and key storage is handled automatically by Cloud.gov. When a FIPS 140-2 validated AWS endpoint is available, Cloud.gov uses it for brokered services. This includes RDS databases and Elasticache Redis. AWS provides a list of FIPS 140-2 validated endpoints. Account information within the training component is associated by email addresses. Training content, including email addresses, quizzes, and quiz results, is stored as relational data in the Cloud.gov brokered RDS Database and is encrypted at rest using AES 256 encryption. The database encryption module provided by Cloud.gov is not FIPS 140 validated.

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?
Cloud Operations makes audit logs available to client organizations and for mutual support in response to security breaches, system and user access, incident reporting and continuous monitoring. Cloud Operations generates and distributes audit reports, provides dashboard access for audited events, and sends audit log data to SIEM and log analysis systems as needed. See AU-2 in the cloud.gov SSP for more details.
Cloud.gov PaaS ensures that all logs outlined in AU-2.a GSPCS Cloud.gov PaaS implementation are recorded in Cloud.gov Cloud Foundry logs.

The GSPCS team coordinates with the GSA IS ISSO, ISSM prior to system changes, after incidents, and yearly to ensure that security relevant logs are available within the cloud.gov tenant application logs.
The GSPCS team will work with the GSA SOC team to ship security relevant web application logs to the GSA SOC for central management and alerting.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Currently the system isn't designed to allow the user to consent or decline; however, if required that function may be deployed prior to deployment.

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.
Right now there is no ability to opt-out; however, if required that function may be deployed prior to deployment. Pleas note if the user opts out then they cannot take the training.

7.2: What are the procedures that allow individuals to access their information?
The user goes to our training website and clicks on Access Past Certificates . The user will be prompted to submit an email address. If the email has been previously stored in the system secure link will be sent to the user's email address. Once the user confirms they have accessed to the email by clicking on the link, the user will have secure access into the system to view their past training certificates.

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.
Currently there is no privacy training available to the user. However, we will have the following banner on our training website to encourage the users to use business/work email addresses instead of personal email addresses.

This is a U.S. General Services Administration Federal Government computer system that is “FOR OFFICIAL USE ONLY.” This system is subject to monitoring. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

We only obtain your information necessary to access this system. We collect information such as agency name and email address, to issue training certificates and for agency reporting management. We carefully protect your information and will not make it available to web tracking software for retention. We do not disclose, give, sell, or transfer any personal information about our visitors, unless required for law enforcement or statute.

To access the GSA SmartPay training system, please use your business or work email only, and not a personal email address

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 program will develop policies around the use of data to ensure the information is used only according to the stated practices in this PIA.