




**Instructions**

**Privacy Impact Assessment (PIA)**

The Privacy Impact Analysis (PIA) questionnaire is applicable to information systems which store or process privacy data. The questionnaire collects information about the types of privacy data which are stored and processed, why it is collected, and how it is handled. A PIA is required based on the results of a Privacy Threshold Analysis (PTA) questionnaire that has been completed for the information system.

Review the following steps to complete this questionnaire:

**1) Answer questions.** Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

**2) Add Comments.** You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.

**3) Change the Status.** You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

**4) Save/Exit the Questionnaire.** You may use any of the buttons at the bottom of the screen to save or exit the questionnaire. The 'Save and Close' button allows you to save your work and close the questionnaire. The 'Save and Continue' button allows you to save your work and remain in the questionnaire. The 'Cancel' button closes the questionnaire without saving your work.

**00 Default Layout** **Workflow Status:** 99 Workflow Complete

**PIA**

**General Information**

<b>PIA ID:</b>	PIA-301	<b>PIA Status:</b>	Completed
<b>Authorization Package (System Name):</b>	SmartPay - Citibank	<b>This is a RPA:</b>	No
<b>Assessment Date:</b>	11/30/2021	<b>Is Latest:</b>	Yes
<b>FISCAL Year:</b>	2021	<b>PIA Required (From Authorization Package):</b>	
<b>Final FISCAL Year:</b>	2021	<b>PIA Expiration Date:</b>	11/30/2022
		<b>Final PIA Expiration Date:</b>	11/30/2022

**Override / Reopen Explanation**

<b>Override FISCAL Year:</b>	2021	<b>Override PIA Expiration Date:</b>	
<b>Reopened Explanation:</b>	Please update this PIA.		

## Other Stakeholders

### Stakeholders (not in Approval Process)

**System Owner (SO):** Shea, David J

**Authorization Official:** Samant, Sagar S

#### System Owner (eMail)

Name (Full)

David Shea

#### Authorization Official (eMail)

Name (Full)

Sagar Samant

### PIA Overview

<b>A.System Name:</b>	A. System, Application, or Project Name:	SmartPay - Citibank
<b>B.Includes:</b>	B. System, application, or project includes information about:	Individuals who apply for and use Federal Government travel and purchase accounts.
<b>C.Categories:</b>	C. For the categories listed above, how many records are there for each?	Travel: 3,499,182 Cards Purchase: 304,400 Cards To be determined Annually
<b>D.Data Elements:</b>	D. System, application, or project includes these data elements:	Name , Contact Information (e.g., address, telephone number, email address) , Social Security Number (SSN) , Permanent Account Number (PAN), Information about individuals provided by third parties (e.g. employer, credit reports,)
<b>Overview:</b>		
<b>PIA-0.1:</b>	Is this a new PIA or Recertification request?	Annual Recertification
<b>PIA-0.1Changes:</b>	If you are reviewing this for annual recertification, please confirm if there are any changes in the system since last signed PIA?	No, Changes

### Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

## 1.0 Purpose of Collection

<p><b>PIA-1.1:</b></p>	<p>What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?</p>	<p>A contractual relationship is in place between Citi and the Federal agencies, and all card accounts for individuals are opened at the request of the agencies. The Citi Commercial Card Service GSA SmartPay3 contract number is GS-36F-GA002. Authority for maintenance of the system includes the following Executive Orders (EO) and statutes: E.O. 9397; E.O. 12931; 40 U.S.C. Sec. 501-502</p>
<p><b>PIA-1.2:</b></p>	<p>Is the information searchable by a personal identifier, for example a name or Social Security number?</p>	<p>Yes</p>
<p><b>PIA-1.2a:</b></p>	<p>If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?</p>	<p>Existing SORN applicable</p>
	<p><b>PIA-1.2 System Of Record Notice (SORN) CR:</b></p>	
<p><b>PIA-1.2 System of Records Notice(s) (Legacy Text):</b></p>	<p>What System of Records Notice(s) apply/applies to the information?</p>	<p>GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program and GSA/GOV-3 Travel Charge Card Program SORNs apply to the information being collected.</p>
<p><b>PIA-1.2b:</b></p>	<p>Explain why a SORN is not required.</p>	
<p><b>PIA-1.3:</b></p>	<p>Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?</p>	<p>No</p>
<p><b>PIA-1.3 Information Collection Request:</b></p>	<p>Provide the relevant names, OMB control numbers, and expiration dates.</p>	
<p><b>PIA-1.4:</b></p>	<p>What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.</p>	<p>In accordance with GSAs contract with Citi, Citi shall maintain electronic records of all transactions for a period of six (6) years after final contract payment. Final contract payment is defined as the final payment for the particular charge under each agency's/organizations task order. Contractors shall provide online access to data (e.g., through the EAS) to GSA and the agency/organization for six (6) years after the occurrence of each transaction. Review/approval and reconciliation data are considered to be parts of the transaction and shall be subject to the same six (6) year record retention requirement. Should an agency/organization decide to use the Contractors EAS as their official record keeping system then the agency's/organizations data, shall be subject to the same six (6) year record retention requirement from the date of creation. Longer transaction record retention and retrieval requirements than those mentioned above may be necessary and will be specified by an agency/organization in task order level requirements.</p>

## 2.0 Openness and Transparency

<b>PIA-2.1:</b>	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
<b>PIA-2.1 Explain:</b>	If not, please explain.	Users are apprised of Citi's privacy policies through Citi's website: <a href="https://www.citigroup.com/citi/privacy.html">https://www.citigroup.com/citi/privacy.html</a> . Additionally, privacy information is provided to users on a yearly basis and may be provided through links in the individual program applications. Lastly, the Citi Chief Privacy Office has established a Privacy Program, which includes a Global Privacy Policy, and jurisdictionally specific privacy policies where required. The Citi privacy program also follows GSA and NIST guidance for PIAs, and ensures that the highest quality of data protection for PII is used and is in accordance with applicable laws and recommendations. According to Citi Privacy and Confidentiality Policy, disclosures regarding the collection, use and sharing of PII and Customer Data must be clear, visible and easily accessible, and available or provided before or at the time of collection of the PII and Customer Data, or as soon after the collection as feasible.


## 3.0 Data Minimization

<b>PIA-3.1:</b>	Why is the collection and use of the PII necessary to the project or system?	Citibank Commercial Cards System (CCCS) is used as a product processor for commercial card transactions. It has a front-end website for cardholders to view their account details and a website for clients to view analytical details for a commercial cards program. All PII collected, such as name, contact information, SSN, etc., is required for the business logic processing, such as, online application, customer email notification, and statement delivery.
<b>PIA-3.2:</b>	Will the system, application, or project create or aggregate new data about the individual?	No
<b>PIA-3.2 Explain:</b>	If so, how will this data be maintained and used?	

<p><b>PIA-3.3:</b></p>	<p>What protections exist to protect the consolidated data and prevent unauthorized access?</p>	<p>Consolidated data is protected through entitlement, role and hierarchy level access. There is restricted access to data files and databases to approved temporary privileged support IDs - access is logged and reviewed. All files are sent and received encrypted with different keys for each client. Unauthorized transfer of information is not allowed. No data is stored on the web servers or DMZ network layer. Data is encrypted in transmission. Data is encrypted at rest in all databases. Clears/cleans objects before reuse in the same application This is tested through extensive ethical hack testing conducted for all applications. Within CCCS, access is restricted only to the data that they are entitled based on the role and customer hierarchy level. Manager approval is required for the entitlement (e.g., role-based access for Citi employees), which is maintained in a central repository called Enterprise Entitlement Review System (EERS). EERS provide detail description of these user entitlements to facilitate entitlement reviews, access revocation and identification of privileged roles within the systems. Business owner, application system owner, and the Information Security Officer are responsible to ensure that all sensitive data is being handled properly. Entitlements for Citi employees are reviewed and updated at least annually.</p>
<p><b>PIA-3.4:</b></p>	<p>Will the system monitor the public, GSA employees, or contractors?</p>	<p>None</p>
<p><b>PIA-3.4 Explain:</b></p>	<p>Please elaborate as needed.</p>	<p>This system does not provide the capability to identify, locate, and monitor individuals. The systems mobile application does not use Location Services.</p>
<p><b>PIA-3.5:</b></p>	<p>What kinds of report(s) can be produced on individuals?</p>	<p>The types of reports that are produced are dependent on the agency. The system has the capability of producing various types of reports, to include account lists, transaction details, and delinquency information (up to and including write-off information). Reports are generally produced in a hierarchical manner, based on the requestors privileges. In this manner, the rollup reports (and search functions) do not generally identify individuals, but do have the ability to drill down to individual records. In this manner, an individual user may be identified.</p>
<p><b>PIA-3.6:</b></p>	<p>Will the data included in any report(s) be de-identified?</p>	<p>Yes</p>
<p><b>PIA-3.6 Explain:</b></p>	<p>If so, what process(es) will be used to aggregate or de-identify the data?</p>	<p>The types of reports that are produced are dependent on the agency. The system does not have the inherent ability to de-identify individuals; however, reports are generally produced in a hierarchical manner, based on the requestors privileges. In this manner, the rollup reports (and search functions) do not generally identify individuals, but do have the ability to drill down to individual records. In this manner an individual user may be identified.</p>

PIA-3.6Why Not: Why will the data not be de-identified?

#### 4.0 Limits on Using and Sharing Information

PIA-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
PIA-4.2:	Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?	Private-Sector Organizations
PIA-4.2How:	If so, how will GSA share the information?	Information is not shared with other Federal, State, Local, agencies. In accordance with Citi Privacy and Confidentiality Policy, Businesses and Global Functions must only share PII and Customer Data with affiliates, Third Parties and other parties to the extent necessary for the fulfilment of the specified or permissible compatible purposes or for compliance with legal and/or regulatory obligations, complaints, investigations or requests and as permitted by applicable laws and regulations. Additional general purpose information regarding Citi and Privacy can be found at: <a href="https://online.citi.com/US/JRS/portal/template.do?ID=Privacy">https://online.citi.com/US/JRS/portal/template.do?ID=Privacy</a>
PIA-4.3:	Is the information collected:	Directly from the Individual
PIA-4.3Other Source:	What is the other source(s)?	Citi collects information directly from the individual to the greatest extent practicable, as well as from the designated Program Administrator, Card System Processor, and employer, as applicable. Businesses and Global Functions that collect PII and Customer Data must disclose to individuals and customers how PII and Customer Data will be collected, used and shared. Businesses and Global Functions must collect, use, and share PII and Customer Data in accordance with its disclosures and with applicable laws and regulations. WAS BOTH only one value allowed
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	Yes
PIA-4.4Who How:	If so, who and how?	Other GSA systems do not have access to the data in the system, but the system shares data dumps into GSA SmartPay Data warehouse. GSA may make permissive disclosures consistent with the routine uses listed in the SORN(s) and shared with other Federal, State, or Local, agencies.
PIA-4.4Formal Agreement:	Is a formal agreement(s) in place?	
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	GSA may make permissive disclosures consistent with the routine uses listed in the SORN(s) and shared with other Federal, State, or Local, agencies.

## 5.0 Data Quality and Integrity

<b>PIA-5.1:</b>	How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?	Citi collects PII directly from the individual to the greatest extent practicable, as well as from the designated Program Administrator, Card System Processor, and employer, as applicable. Citi checks for and corrects as necessary, any inaccurate or outdated PII used by its systems; and, issues guideline ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. The system validates field edit checks for proper data entry, format and required/not required edit checks, by the users or Program Administrators. Programmatic checks are done on the data fields received in the files, such as, numeric data for phone numbers. Completeness of each record within the files are checked by file format type.
-----------------	--	---

## 6.0 Security

<b>PIA-6.1a:</b>	Who or what will have access to the data in the system, application, or project?	Access to the system is limited to cardholders, Customer Program Administrators (GSA employees or contractors), and limited Citi personnel with the proper entitlements based on their role and corporate client hierarchy level.
<b>PIA-6.1b:</b>	What is the authorization process to gain access?	With regard to Citi personnel, access is restricted only to the data that they are entitled based on the role and customer hierarchy level. Manager approval is required for the entitlement, which is maintained in a central repository called Enterprise Entitlement Review System (EERS). EERS provide detail description of these user entitlements to facilitate entitlement reviews, access revocation and identification of privileged roles within the systems. Business owner, application system owner, and the Information Security Officer are responsible to ensure that the privacy data is being handled properly. Entitlements are reviewed and updated at least annually. In general, only customer service representatives, upon request by the cardholder, and system administrators, in the management of the underlying system, have access to CCCS data.
<b>PIA-6.2:</b>	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
<b>PIA-6.2a:</b>	Enter the actual or expected ATO date from the associated authorization package.	6/29/2022

<b>PIA-6.3:</b>	How will the system or application be secured from a physical, technical, and managerial perspective?	All system resources and access are controlled via user entitlements. User entitlements are checked at least annually by applicable managers. Extensive ethical hack testing is conducted for all applications. Unauthorized transfer of information is not allowed. No data is stored on the web servers or DMZ network layer. Data is encrypted in transmission. All sensitive fields will be encrypted in the database. Clears/cleans objects before reuse in the same application. All critical PII data is masked on the screen. Citi performs daily incremental and weekly full backup of system information. Data Center building access has single entry controlled by man traps. Data Center employee access controlled by a combination or badge reader, biometric hand reader, and iris scanner as applicable. Visitors must go through a separate man trap and sign in at the security desk. Data Center security guards onsite, on duty, 24/7, monitor all security cameras and alarms from a security control center. Physical access logs are reviewed monthly; inventories of all critical equipment, including access devices are performed quarterly
<b>PIA-6.4:</b>	Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?	Yes
<b>PIA-6.4What:</b>	What are they?	Citi has multiple programs in place to identify suspected or confirmed security incidents and breaches. The system undergoes periodic security scans to detect vulnerable software. There are ongoing reviews of system audit logs to detect abnormal system conditions. Citi has a fraud detection program that is used to detect and respond to suspected fraudulent uses of cards. In addition to real-time monitoring of all external IPs via IDS, Citi's Citigroup Threat Assessment Center (CTAC) group monitors the IDS alerts, records suspicious activity in tickets and escalates them to the Intrusion Detection and Vulnerability Analysis (IDVA) group that takes further action to address them according to established procedures.

## 7.0 Individual Participation

<b>PIA-7.1:</b>	What opportunities do individuals have to consent or decline to provide information?	The GSA IT Security Policy and GSA requirements for PIAs, SORNs, Privacy Act Statements, Annual Reviews of system notices ensure that GSA limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice for which the individual has provided consent. GSA cannot deny a legal right, benefit, or privilege if individuals refuse to provide their SSN unless the law requires disclosure or, for systems operated before 1 January 1975, a law or regulation adopted prior to that date required disclosure in order to verify the identity of the individual.
<b>PIA-7.1Opt:</b>	Can they opt-in or opt-out?	Yes



<p><b>PIA-7. 1 Explain:</b></p>	<p>If there are no opportunities to consent, decline, opt in, or opt out, please explain.</p>	<p>An agency can only make collection from GSA mandatory when a Federal statute, executive order, regulation, or other lawful order specifically imposes a duty on the person to provide the information; and the person is subject to a specific penalty for failing to provide the requested information. The effects, if any, of not providing the information “ for example the loss or denial of a privilege, benefit, or entitlement sought as a consequence of not furnishing the requested information. According to Citi Privacy and Confidentiality Policy, Businesses and Global Functions must collect and use only as much PII and Customer Data as is reasonably necessary or appropriate to provide products and services or as disclosed. Disclosures regarding the collection, use and sharing of PII and Customer Data must be clear, visible and easily accessible, and available or provided before or at the time of collection of the PII and Customer Data, or as soon after the collection as feasible. Individuals may request not to receive marketing material or solicitations and to receive marketing communications via their preferred channels (e.g., email, phone, text messages, etc.) to the extent feasible and in accordance with applicable laws and regulations. This includes opting out of marketing solicitations but does not preclude communications that are required to perform Citi’s contractual, legal or regulatory responsibilities. Businesses and Global Functions must comply promptly with marketing opt-out requests in consultation with Legal, Compliance and/or regulatory authorities as required.</p>
<p><b>PIA-7.2:</b></p>	<p>What are the procedures that allow individuals to access their information?</p>	<p>Individuals have the ability to access their PII maintained in GSA system(s) of records. GSA publishes CFR Part 105-64 GSA Privacy Act Rules, which governs how individuals may request access to records maintained in a Privacy Act system of records. GSA also provides access procedures in system of records notices and adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act Requests. According to Citi Privacy and Confidentiality Policy, Businesses and Global Functions must honor customer communication preferences, access requests and correction requests to the extent provided by law or regulation. Where provided by applicable laws and regulations, individuals may upon proper authorization request access to their PII in a form permissible under applicable laws and regulations. Additionally, cardholders may request access to their data by contacting a Citi customer service representative</p>
<p><b>PIA-7.3:</b></p>	<p>Can individuals amend information about themselves?</p>	<p>Yes</p>

**PIA-7.3How:**

How do individuals amend information about themselves?

GSA provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and, establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners, and where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. More information about PII redress can be found in CFR Part 105-64 GSA Privacy Act Rules. Citi allows individuals to participate in the management of their PII where legally required. The amendment is carried out by the AOPC or the CAS as applicable. According to Citi Privacy and Confidentiality Policy, Businesses and Global Functions have a shared responsibility with customers and staff to keep PII and customer data accurate and up-to-date. Businesses and Global Functions must honor customer communication preferences, access requests and correction requests to the extent provided by law or regulation. Where provided by applicable laws and regulations, individuals may upon proper authorization, review the accuracy of their PII and, where appropriate or legally required, request to have it corrected, completed or amended. Business owner, application system owner, and the Information System Security Officer are responsible to ensure that the privacy data is being handled properly. User access is restricted only to the data that they are entitled based on the role and customer hierarchy level. Misuse of data by those having access is reinforced by entitlement, and any violation is reported. Updates to confidential PII data are logged IAW Citi Information Security Standards (CISS).

## 8.0 Awareness and Training

<b>PIA-8.1:</b>	Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.	GSA regularly updates its IT Security Awareness and Privacy Training and Privacy Training 201, a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities. All GSA account holders electronically sign the GSA Rules of Behavior before taking privacy training exit exams. GSA privacy training includes targeted role-based privacy training for personnel having responsibility for PII and ensures that personnel certify acceptance of responsibilities for privacy requirements. The Citi Chief Privacy Office (CPO) is responsible for creating and maintaining a training and awareness framework which serves to increase awareness of Privacy and Confidentiality-related requirements and obligations and promoting a culture of compliance and control. This includes developing and maintaining a global high-level Privacy and Information Compliance training as well as ensuring that relevant global, regional, business and country-level trainings include privacy sections as appropriate. The CPO also develops and maintains oversight routines regarding CPO-owned training.
-----------------	--	---

## 9.0 Accountability and Auditing

<b>PIA-9.1:</b>	How does the system owner ensure that the information is used only according to the stated practices in this PIA?	Systems are periodically audited and assessed for security weaknesses, and the resulting Security Assessment Reports and POA&M are developed to monitor privacy controls and internal privacy policy to ensure effective implementation. These POA&Ms are provided to GSA on a quarterly basis. Additionally, for CCCS, the Citi business owner, application system owner, and the Information Security Officer are responsible to ensure that the privacy data is being handled properly. Citi's Global Privacy Committee (GPC) meets at least quarterly, and provides oversight and governance over the Program. Among the responsibilities of the GPC include reviewing Corrective Action Plans (CAPs), Internal Audit reports, Compliance Testing reports and regulatory findings.
-----------------	---	--