## 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: 523
System Name: SmartPay - Citibank
CPO Approval Date: 1/14/2026
PIA Expiration Date: 1/13/2029

## Information System Security Manager (ISSM) Approval

Arpan Patel

## System Owner/Program Manager Approval

## Chief Privacy Officer (CPO) Approval

Richard Speidel

## PIA Overview

**A:** System, Application, or Project Name:
SmartPay - Citibank

**B:** System, application, or project includes information about:
Individuals who apply for and use Federal Government travel and purchase accounts.

**C:** For the categories listed above, how many records are there for each?

Travel: 2,772,401 Cards Purchase: 424,242 Cards To be determined Annually

**D:** System, application, or project includes these data elements:
Personal Identity and Authentication Information - 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,) Travel, Helpdesk Services, Reporting Information, Payment Information.

## Overview:

Citi provides a comprehensive suite of web-based tools and financial EDI interfaces to allow customers to configure a solution that meets their organization's objectives. Enhanced and Level 3 data are the cornerstones of Citi's electronic capability.

Citi's Electronic Access Systems (EAS) are built using a modular approach that provides maximum flexibility. The core of Citi's system architecture is the Global Data Repository (GDR). Citi's GDR is a warehouse of global transaction and demographic data. It is complemented by enhanced data feeds, be it Level 2 or Level 3 data, hotel folio data, or other data streams to Citi clients' purchase information. GDR feeds Card Management and Data-mining tools with clients purchase information.

Citi's Citi Solution Delivery Life Cycle (CSDLC) Standard process governs how Citi establishes and maintains their technology tool set. This disciplined approach leads to electronic capabilities that meet Citi clients' objectives to ensure data security is maintained and applications contain the feature functionality requested. An important input into the process is feedback and knowledge sharing exchanged via the Technology Advisory Group (TAG).

A business intelligence engine provides users with the ability to use predefined reports and design their own queries to meet the GSA SmartPay®3 requirements. Data can be displayed in table and graphical (pie charts, bar graphs) formats. Over 650 data elements are available for users to query on and create their custom reports.

Access control is managed in a hierarchy model using a role-based entitlement approach that makes user administration easy and efficient. Card management and reporting capabilities are only accessible to users with the correct entitlement. CCCS covers the following functions:

□

CitiManager, is used by Commercial Cards customers globally to access card demographic, transaction, and statement information. Online application and maintenance of card holder and non-card holder administration are key features of the system, which enable corporate Program Administrators to effectively manage their card program for their employees. This is the central portal for the CCCS linking various other related Commercial Cards systems through Single Sign On capability, i.e., CCRS and CCMS. Additionally, CSAP is the orchestration tool providing CitiManager with a channel for biometric authentication and risk engine (Auth Control Engine) via SaaS provider "Threat Metrix". It supports knowledge-based authentication "Secret Questions". SMS is processed through CitiManager via "SINCH", and Voice is processed through Citi Multi Factor Authentication (CitiMFA) via external 3rd party supplier "PROVE".

□ CitiDirect Card Management System (CCMS) is a comprehensive Internet-based program that offers account set-up and management, rapid data delivery, and essential service functions. In its fullest use, the CCMS supports multi-level electronic workflow approval and re-allocation capabilities that seamlessly integrate with financial systems. The system provides a single access point for Program Administrator(s) to perform and maintain program management, transaction review, allocation, and reconciliation.

□ Citi Custom Reporting System (CCRS) enables Program Administrator(s) to access, navigate, and explore relational data to make key business decisions in real time. Key features of the CCRS include over 650 data elements, including Level 3 and enhanced folio data available for report customization. Report customization features include: download capabilities supporting spreadsheets, PDF, and word processing formats; pre-scheduled and ad hoc reporting capabilities; advanced features such as filtering, column calculation using an expression editor, creation of custom prompts, and on-the-fly charting capabilities.

□ Citi Manager Mobile app (CMM) is used by Commercial Cards customers globally to utilize their smart phone to access key Citi Manager account data. CMM is the mobile app channel for the Citi Manger application, with limited functionality compared to the Citi Manager Portal. Customers can view statement information, balances, available credit, card activation, and reporting of lost/stolen credit cards. Enhanced security measures include biometric authentication and one-time password (OTP) for login.

Smart Disputes (SD) is an internal facing application used by Citi internal Commercial Cards call-center agents to manage disputes on card transactions with TSYS, VISA and MasterCard. The application pulls transactions from TSYS, Cards system of reference and creates Disputes with VISA and MasterCard leveraging the appropriate association rules. The application submits the disputed transactions to the associations and provides updates to

TSYS. When associations reply, the application will update the disputed transaction case with the appropriate information.

 Proactive Accurate Controlled and Timely (PACT-GSA) is an internal facing, global client centric service platform for support teams. This B2B application is used by Citi internal Commercial Cards customer service and operations units to track, research, and resolve exceptions and customer inquiries. The core Pegasystems is vendor-built, with Citibank staff responsible for the enhancement, maintenance, and support of the implementation.

 Illumio ASP (Adaptive Security Platform) is a distributed software platform designed to continuously protect communications within and across tiers of applications, wherever they are running. It creates secure and granular network segmentation to compartmentalize workloads and applications, reducing the attack surface exposed to cyber vulnerabilities. Illumio is bifurcated into both the Full ATO boundary (Zone 1) and the Secondary Security Boundary (Zone 2). The Policy Compute Engine (PCE) and the Illumio Self-Service Dashboard resides in Zone 2. The Virtual Enforcement Node (VEN) and Activated Policies reside in Zone 1.

The PCE is the Enterprise, central management platform, responsible for all analysis, policy management, configuration, and user interaction. TCP 8444 is used by PCE to send messages (referred to as lightning bolts) to the VEN. PCE access is restricted to Illumio Administrators. The Illumio Self-Service Dashboard is a Graphical User Interface (GUI) that uses the Illumio API to communicate with the PCE. The Self-Service Dashboard is used by DevOps personnel to configure the VEN agents installed on the application servers in Zone 1. DevOps personnel write the application server specific ingress and egress policies based on analysis of the network telemetry report, which is generated by information collected by the agents and shows all the traffic communication to and from a specific server. Shared/Enterprise services have integrated policies pre-built for use by applications which are supported by these tools, removing the need for each individual DevOps team to collect required policy details to ensure required communications from standard enterprise technology and security tools. Enforcement of the policies creates a unique, micro-segmented environment that deploys a controlled trust security strategy. To ensure stability and effectiveness, any changes to the rule sets are tested in the lower environments prior to moving to enforcement in the production environment. Once enforcement is implemented, rules will pass to the respective agents to allow or disallow traffic and enable network segmentation for the Zone 1 servers. Submission of changes in the self-service dashboard triggers a process where a Change Request is raised, which requires approval from the respective application managers prior to rule being moved from Illuminate (Test) to Enforcement mode. There is also an annual review and attestation performed by the Application Teams.

The VEN is a lightweight agent, multiple-process application with a minimal footprint that runs on a workload. The VEN manages firewalls at an OS level and is installed on every GSA server in the CCCS environment except IBM Mainframe. The VEN is responsible for providing telemetry data (flow / process data) to PCE and enforcing policy via a host-based firewall (IP tables, Windows Filtering). Micro-Segmentation Policies are stored on the host server. TCP 8443 is used by the VEN agent to send heartbeats, and to send and request information. Only port, protocol, service connectivity data is sent between PCE and VEN, no PII data is shared. The VEN agent initiates all connections to PCE. PCE will notify VEN of any changes to the policies which are enforced and activated at the workload. The VEN performs the following additional tasks: Interacts with the native networking interfaces to collect traffic flow data. Enforces policy received from the PCE. Summarizes the collected traffic-flow data, then reports it to the PCE. Sends heartbeats to the PCE. The VEN extracts and reports workloads system information status', such as network interfaces, and listening processes, to the PCE. The PCE (Zone2) computes a unique security policy for each managed workload and transmits it to the VEN. When the VEN is finished programming a firewall for each workload, it reports back to the PCE. The PCE then considers these workloads as having a synced policy.

## 1.0 Purpose of Collection

**1.1:** What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
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

**1.2:** Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

**1.2a:** If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

**1.2: System of Records Notice(s) (Legacy Text):** What System of Records Notice(s) apply/applies to the information?
GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program and GSA/GOV-3 Travel Charge Card Program SORNs apply to the information being collected.

**1.2b:** Explain why a SORN is not required.
An agency is generally only required to modify a SORN when there is a "significant change" in the way the system of records operates.

**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.
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.

## 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.
Users are apprised of Citi's privacy policies through Citi's website: "https://www.citigroup.com/citi/privacy.html". 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

**3.1:** 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.

**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?
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.

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

**3.4 Explain:** Please elaborate as needed.
This system does not provide the capability to identify, locate, and monitor individuals. The systems mobile application does not use Location Services.

**3.5** What kinds of report(s) can be produced on individuals?
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.

**3.6** Will the data included in any report(s) be de-identified?
Yes

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

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

## 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?
Private-Sector Organizations

**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: https://online.citi.com/US/JRS/portal/template.do?ID=Privacy

**4.3:** Is the information collected:
Directly from the Individual

**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

**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?
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.

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

**4.4NoAgreement:** 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

**5.1:** 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

**6.1a:** 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.

**6.1b:** 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.

**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.
6/20/2025

**6.3:** 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

**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?
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, Citis 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

**7.1:** 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.

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

**7.1Explain**: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
**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.**

**7.2:** What are the procedures that allow individuals to access their information?

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

**7.3:** Can individuals amend information about themselves?
Yes

**7.3How**: How do individuals amend information about themselves?
Request for records for Privacy Act.

## 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.
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

**9.1:** 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. Citis 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.