GSA SmartPay® - Citibank

Privacy Impact Assessment

04/24/2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

Table of contents

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)?

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

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

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 for the information system(s) supporting the project?

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

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline 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?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about Citibank Commercial Cards System (a.k.a. GSA SmartPay® – Citibank). The Citibank on behalf of GSA will 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

GSA SmartPay - Citibank

System, application or project includes information about

- Individuals who apply for and use Federal Government travel and purchase accounts.

System, application or project includes

- 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, background investigation (BI). Please note that the GSA SmartPay master contract requires the contractor bank to get background investigation on all of their personnel working on the GSA SmartPay contract. The credit worthiness is a part of the BI process.*)*

Overview

The GSA SmartPay - Citibank (a.k.a. Citibank Commercial Cards System/CCCS) is a comprehensive suite of web-based tools and Financial Electronic Data Interchange (EDI)

interfaces that allow customers to configure a solution that meets their organization's objectives for credit card issuance and management. 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 is required for the business logic processing such as, online application, statement delivery, and customer email notification.

Data elements maintained in CCCS include demographic information of cardholder such as, name, address, phone number, email address, SSN, PAN, employer, and credit card processor. Additional information includes, account processing and management information, including purchase authorizations and vouchers, charge card applications, charge card receipts, terms and conditions for card use, charge card transactions, contractor monthly reports showing charges to individual account numbers, account balances, and other data needed to authorize, account for, and pay authorized purchase card expenses.

Access to these data is determined by entitlement based on role, corporate client hierarchy level, and manager approval. Only the cardholder, Customer Program Administrators, Citi employees including Citi Jacksonville operations and account management team, with proper entitlements has access to the data.

GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program and GSA/GOV-3 Travel Charge Card Program SORNs apply to the information being collected.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

GSA is collecting this data in order to establish and maintain a system for operating, controlling, and managing a charge card program involving commercial purchases by authorized Federal Government employees and contractors. The program provides both plastic and virtual cards for Fleet cards, Integrated cards, and Tax Advantage cards.

The PII collected and used is the same information as that utilized for major credit cards. All PII collected is required for the business logic processing, such as, online application, customer email notification, and statement delivery.

1.2 What legal authority and/or agreements allow GSA to collect 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

1.3 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 being collected?

Data is retrieved by Card or Account number, employee ID (if provided by the agency), and the name. GSA/GOVT-6 applies to the information being collected.

1.4. Has any 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.

This is not applicable to Citibank Commercial Card System. An ICR has not been submitted to or approved by OMB.

1.5. 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.

In accordance with GSA's 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/organization's 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 Contractor's EAS as their official record keeping system then the agency's/organization's 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.[1]

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

A privacy risk has not been determined for the purpose of the collection. Citi employs privacy professionals within the Chief Privacy Office and privacy accountability is embedded throughout the organization in the first and second lines of defense, with identified in-business privacy officers and business unit compliance officers to meet its compliance obligations with regard to privacy and to proactively identify and mitigate any privacy risk.

All PII collected is required for the business logic processing. The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected. All critical PII is masked on the screen. The system reinforces entitlement to protect unauthorized access, and any violation is reported.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? 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

[1] GSA SmartPay 3 Master Contract: https://smartpay.gsa.gov/content/about-gsa-smartpay#a2
See the "GSA SmartPay 3 Master Contract Terms and Conditions" Section C.7.2.4.

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.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

There are no specific privacy risks for the system that relate to openness and transparency. 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.

In accordance with the Transparency principle, Citi discloses its online and offline data collection and use practices to its customers in a variety of contexts. For example, Citi sends annual Privacy Notices for its U.S. Consumer businesses in accordance with the requirements of Gramm-Leach-Bliley Act and Regulation P: Privacy of Consumer Financial Information (12 CFR 216). Citi also posts online privacy policies on its websites and mobile apps.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

- GSA employees and contractors who apply for and use Federal Government travel and purchase accounts.

3.2 What PII will the system, application or project include?

- 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, background investigation)

Data is retrieved by Card or Account number, employee ID (if provided by the agency), and the name. All PII collected is required for the business logic processing, such as, online application, customer email notification, and statement delivery. All critical PII is masked on the screen. The system reinforces entitlement to protect unauthorized access, and any violation is reported.

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

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.

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

The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

- Consolidated data is protected through entitlement, role and hierarchy level access
- 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.

3.6 Will the system monitor the public, GSA employees or contractors?

This system does not provide the capability to identify, locate, and monitor individuals. The system's mobile application does not use "Location Services."

3.7 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 requestor's 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.

3.8 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?

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 requestor's 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.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

Citi limits the collection and retention of PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; 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; and, conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holding, at least annually, to ensure that only PII identified in the notice is collected and retained. Social Security Numbers (SSNs) are not collected unless a credit worthiness check is required, and SSNs are not made available to the GSA Agency/Organization Program Coordinator (A/OPC).

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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?

Citi follows GSA privacy policy and guidance in conducting the Privacy Impact Assessment of the system and developing the PIA. In order to provide cardholder services and organizational management of cardholders, Citi identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection. Citi limits the collection and retention of PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; 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; and, conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holding, at least annually, to ensure that only PII identified in the notice is collected and retained.

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?

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 or is it taken from another source? If so, 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.

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

Other GSA systems do not have access to the data in the system, or share data. Information is also not shared with other Federal, State, or Local, agencies.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

A privacy risk has not been determined in regards to use limitation. The use and sharing of any data is in accordance with the card service agreement.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected 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.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

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. To the extent possible, Citi checks for and corrects as necessary, any inaccurate or outdated PII used by its systems; and, issues guidelines 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. Oftentimes, it is the cardholder that provides updated or incorrect information to Citi via a customer service representative or through other means.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

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?

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.

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 GSA completed a system security plan for the information system(s) or application?

A System Security Plan (SSP) was submitted by the bank as a part of their Assessment & Authorization (A&A) package for SP3. GSA continues to work with the bank to address the open issues and the SSP will be updated as a part of the overall A&A package submission, which will be updated based on additional testing and artifact collection.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

- All system resources and access are controlled via user entitlements
- User entitlements 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 perform 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 reviewed monthly; inventories of all critical equipment, including access devices, performed quarterly

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

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

There are inherent residual risks in most systems. In systems that contain PII, these risks could pose some risks to the underlying data. To mitigate these risks, the system has been engineered in accordance with NIST security and privacy control guidance, and has been assessed against those controls. The system has been granted an authority to operate, indicating that any inherent risks were deemed by the Authorizing Official (AO) to be acceptable and reasonable. During its lifetime, the GSA Smartpay - Citibank system goes through vulnerability scans on a quarterly basis and a Plan of Action and Milestone (POA&M) is required to address vulnerability risks that cannot be fully resolved on a timely manner. Additionally, Citi also, implements new security controls where appropriate to improve its risk posture.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

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.

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 procedures 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? If so, how?

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).

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

A privacy risk has not been determined in regards to individual participation. 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, carried out by the AOPC or the CAS as applicable. Business owner, application system owner, and the Information Security Officer are responsible to ensure that the privacy data is being handled properly. 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).

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

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.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

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. The CPO work with the Lead In-Business Privacy Officers (IBPO) and other appropriate stakeholders to determine if additional targeted training is required for any areas or roles within Citi Businesses and Global Functions. All Citi personnel that have access to customer information, including Citi customer service personnel are mandated to take the Citi-provide training in the protection of customer information and privacy data.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with 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) meet 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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

There are no current system risks associated with accountability and auditing. These controls are part of a continuous monitoring process that re-evaluates controls throughout the system's lifecycle.

---

[1] OMB Memorandum *Preparing for and Responding to a 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.