




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

PIA ID:	PIA-302	PIA Status:	Completed
Authorization Package (System Name):	SmartPay - US Bank	This is a RPA:	No
Assessment Date:	11/15/2021	Is Latest:	Yes
FISCAL Year:	2021	PIA Required (From Authorization Package):	
Final FISCAL Year:	2020	PIA Expiration Date:	11/15/2022
		Final PIA Expiration Date:	11/15/2022

Override / Reopen Explanation

Override FISCAL Year:	2020	Override PIA Expiration Date:	
Reopened Explanation:	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

A.System Name:	A. System, Application, or Project Name:	SmartPay - US Bank
B.Includes:	B. System, application, or project includes information about:	Access Online: Federal employees and contractors (US Bank staff) Voyager Fleet / Other the Road (OTR): Federal employees and contractors (US Bank staff) Syncada: Federal employees and contractors (US Bank staff)
C.Categories:	C. For the categories listed above, how many records are there for each?	277,847 US Bank Purchase cards and 195,187 Travel Cards for unique federal employees as of June 2020.
D.Data Elements:	D. System, application, or project includes these data elements:	The following information is collected from public users: None. The following information is collected from the federal government: To establish/open centrally billed accounts, cardholders name, business address and telephone numbers are obtained. To establish/open an individually billed travel accounts cardholder personally identifiable information (PII) obtained is full name, home or business address, date of birth, telephone number, and if a cardholder agrees to creditworthiness checks, their social security number (SSN).
Overview:		
PIA-0.1:	Is this a new PIA or Recertification request?	Annual Recertification
PIA-0.1Changes:	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

PIA-1.1:	What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate 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. A contractual relationship is in place between U.S. Bank and the Federal agencies, and all card accounts for individuals are opened at the request of the agencies. The US Bank Commercial Card Service GSA SmartPay3 contract number is GS-36F-GA0001. 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.
PIA-1.2:	Is the information searchable by a personal identifier, for example a name or Social Security number?	Yes
PIA-1.2a:	If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?	Existing SORN applicable
	PIA-1.2 System Of Record Notice (SORN) CR:	
PIA-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.
PIA-1.2b:	Explain why a SORN is not required.	
PIA-1.3:	Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?	No
PIA-1.3 Information Collection Request:	Provide the relevant names, OMB control numbers, and expiration dates.	

PIA-1.4:	What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.	<p>In accordance with GSAs contract with U.S. Bank, U.S. Bank 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/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.</p> <p>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/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


PIA-2.1:	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
PIA-2.1 Explain:	If not, please explain.	<p>Master Contract requirements prohibit U.S Bank from sharing cardholder PII outside of the purposes of GSA and Agencies to manage the GSA SmartPay program. Access Online: Information is traditionally entered either by an Agency/Organization Program Coordinator (A/OPC) or via integration with clientsâ€™ system via web service. The only time a user enters their data is when an agency decides to utilize function to send email to users to request they enter their own information via cardholder initiated setup (CIS). The cardholder receives two emails when CIS is used and the option to send directly to the cardholder is chosen. The other flavor of CIS is to send the manager an email with a link and a separate email with the code. Upon entering the information, the manager is brought to a screen asking for email addresses of cardholders who need to be sent requests to submit their own demographic information. Either flavor â€œ ultimately cardholders enter and submit their own demographic information. Voyager: No, we do not share information about individuals PII. Syncada: We do not share personal data with any organization outside US Bank.</p>

3.0 Data Minimization

PIA-3.1:	Why is the collection and use of the PII necessary to the project or system?	The collection of all identified PII data is necessary to verify identity and risk as required for servicing and regulatory (Office of Foreign Assets Control/OFAC) requirements. The following information is collected from public users: None. Information is collected from federal government employees only: To establish/open centrally billed accounts, cardholders name, business address and telephone numbers are obtained. To establish or open an individually billed travel account, the cardholder PII that is obtained is full name, home or business address, date of birth, telephone number, and if a cardholder agrees to creditworthiness checks, their SSN
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	No
PIA-3.2 Explained:	If so, how will this data be maintained and used?	
PIA-3.3:	What protections exist to protect the consolidated data and prevent unauthorized access?	The system follows NIST Moderate System Security Requirements for DATA at rest and on transit. The system controls are assessed every 3 years by an independent assessor per NIST standards. In addition a set of critical controls are assessed annually and scans are evaluated every 3 months and findings monitored and resolved within SLA.
PIA-3.4:	Will the system monitor the public, GSA employees, or contractors?	None
PIA-3.4 Explain:	Please elaborate as needed.	This system does not provide the capability to identify, locate, and monitor individuals.
PIA-3.5:	What kinds of report(s) can be produced on individuals?	The applications have User List Reports that show the types of access the user has in the system that can be run by A/OPCs and internal users with correct access. It does include some contact information like address and phone number. Transaction reports can be run that would have cardholder name (or vehicle number), merchant/supplier name, dollar amount of transaction.
PIA-3.6:	Will the data included in any report(s) be de-identified?	No
PIA-3.6 Explain:	If so, what process(es) will be used to aggregate or de-identify the data?	

PIA-3.6Why Not:	Why will the data not be de-identified?	Summary (aggregate) level data is available in reporting that allows the A/OPC to exclude cardholder information. US Bank 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).
------------------------	-----------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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?	None
PIA-4.2How:	If so, how will GSA share the information?	N/A
PIA-4.3:	Is the information collected:	Directly from the Individual
PIA-4.3Other Source:	What is the other source(s)?	US Bank collects information directly from the individual cardholder to the greatest extent practicable, as well as from the designated Program Administrator and A/OPC's, Card System Processor via integration with client's system via web service, and employer (Federal Agency customer), as applicable. Please see response to section 2.1 for additional details
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?	A formal agreement is in place with Total Systems (TSYS) outside of GSA to ensure PII information is secure. All information passed between U.S. Bank and TSYS is relayed through a persistent connection; USBank initiates requests to TSYS via MQ Series or sends via web service through dedicated T1 lines to ensure requirements are met in the formal agreement of data transfer.
PIA-4.4Formal Agreement:	Is a formal agreement(s) in place?	
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	

5.0 Data Quality and Integrity

PIA-5.1:	How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?	The federal government is responsible for verifying data accuracy and completeness. The system does not have built in controls to verify accuracy. US Bank collects PII directly from the individual to the greatest extent practicable, as well as from the designated A/OPCs, Card System Processor, and employer (Federal agency customer), as applicable. The system validates field edit checks for proper data entry, format and required/not required edit checks, by the users or A/OPCs. 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. If incomplete information to establish an account is encountered, the request will be rejected and returned to the A/OPC.
-----------------	------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6.0 Security

PIA-6.1a:	Who or what will have access to the data in the system, application, or project?	US Bank Administrative Users,, U.S. Bank personnel tasked with administration of GSA data on the US Bank system. GSA Administrative Users GSA/Agency personnel tasked by roll to access and review their Agency data per contract and task order. US Bank Database Administrators, U.S. Bank personnel US BANK Production Support Staff
PIA-6.1b:	What is the authorization process to gain access?	The access is role based defined and granted based on contract and Task Order requirements. When no longer needed access via role is removed within established rules. US Bank provides documents annually to verify the access controls are followed.
PIA-6.2:	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
PIA-6.2a:	Enter the actual or expected ATO date from the associated authorization package.	1/14/2020

PIA-6.3:

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

U.S. Bank verifies individual access authorizations before granting access to the facility. U.S. Bank enforces physical access control by use of guards, badge access readers, keys, combinations, alarm contacts, and CCTV at all physical access points to the facility where the SmartPay " US Bank System resides. U.S. Bank changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated. Access to high-security zones by individuals who have not been issued physical access credentials must be limited to business need, and these individuals must be escorted by authorized personnel at all times. U.S. Bank enforces user identification and passwords including multi-factor authentication on privileged accounts. Periodic security audits are conducted on a regular basis for the applications and devices that encompass GSA SmartPay " US Bank. U.S. Bank uses the internal ISS (Information Systems Security) department for regular monitoring of users, backup of sensitive data, etc. Coordination of physical, technological, and managerial controls is managed between U.S. Bank's teams within TOS (Technology Operations Services), and ISS (Information Security Services).

Yes

PIA-6.4:

Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?

PIA-6.4What:

What are they?

Incidents are discovered in several different internal processes including personnel reporting suspicious activity as well as events identified using the Security Incident Event Manager (SIEM) tool to identify anomalies within the devices across the enterprise logging and monitoring. Once an event is escalated it becomes an Incident and tracked. Each information security incident will be categorized based on the threat level below. If an information security incident is a severity level 1 or 2, an emergency declaration will be made. Any deviation from U.S. Bank policies, standards, and supporting plans, and all procedures/processes involved with the timely resolution of an information security incident will be tracked. If an information security incident is a severity level 1 or 2, the CSIRT IC will ensure changes are noted. All incidents are managed based on their categorization level and worked to closure within the timeframe relevant to the incident identified in the U.S. Bank Incident Response Plan. Each information security incident will be assessed for its severity and potential impact to U.S. Bank's assets (breach of PII involving the system, application, or project), and the appropriate action will be agreed upon by the CSIRT (Computer Security Incident Response Team) before responding. The four security levels are defined as: Severity 1 " Critical: An incident with severe and lasting system impact, large number of users or customers compromised or affected imminent threat of destructive attack, or damaging publicity to U.S. Bank is certain. Severity 2 " High: An incident with significant system impact, large number of users or customers compromised or affected, highly likely threat of destructive attack, or damaging publicity to U.S. Bank is probable. Severity 3 " Medium: An incident with moderate system impact, moderate number of users or customers compromised or affected, threat of destructive attack is likely, or damaging publicity to U.S. Bank is likely. Severity 4 " Low: An incident with minor system impact, small number of users or customers compromised or affected, threat of destructive attack is remote, or damaging publicity to U.S. Bank is unlikely. After discovery of a potential breach, U.S. Bank shall immediately notify (within one hour) the designated GSA and Agency personnel by telephone or e-mail so that U.S. Bank may take appropriate action. Initial report of a breach shall be followed by a formal notification in writing within five (5) business days after detection of the breach. U.S. Bank shall be responsible for making all determinations related to the privacy breach mitigation activities, including any necessary notifications to potentially affected individuals, Federal agencies, or external oversight organizations

PIA-7.1:	What opportunities do individuals have to consent or decline to provide information?	<p>The GSA IT Security Policy and GSA requirements for PIAs, SORNs, Privacy Act Statements, 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. Consent to Credit Worthiness must be exercised for the Individually Billed Travel Card. Agencies must make decisions on those cases where employees are opting out. 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.</p>
PIA-7.1Opt:	Can they opt-in or opt-out?	Yes
PIA-7.1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	
PIA-7.2:	What are the procedures that allow individuals to access their information?	<p>Access Online allows individuals web-based access to their account information with a userID and password to facilitate payments and updates on PII data. Fleet Commander Online allows fleet managers and A/OPC’s web-based access to update vehicle or cardholder information to update account addresses and phone numbers.</p>
PIA-7.3:	Can individuals amend information about themselves?	Yes
PIA-7.3How:	How do individuals amend information about themselves?	<p>Individuals cannot delete their records from the system. 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. 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.</p>

8.0 Awareness and Training

PIA-8.1:

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

U.S. Bank staff with access to customer PII information are bound by information security policies that are accessible to all employees on the internal corporate web portal and U.S. Bank holds all personnel accountable for understanding and complying with those policies. All U.S. Bank employees, contractors and associates are trained on their applicable information security responsibilities and required to attest to their commitment to carry out their information security roles and responsibilities. Employees are also required to take information security training within their first 30 days on the job. Courses are automatically assigned pursuant to the employee's role, and monitored for completion. U.S. Bank's Code of Ethics and Business Conduct is reviewed during the new employee orientation session and the Code includes information security requirements. Employees are required to complete the Code of Ethics and Business Conduct on-line training within their first 30 days of employment and are required to recertify on an annual basis. The complete Code of Ethics and Business Conduct are located on the U.S. Bank Intranet site, and employees are encouraged to read and understand how the Code applies to them. Employees are also informed of the Ethics Hotline should they feel someone is in violation of the Code. Complaints made to the Ethics Hotline are taken very seriously and an investigation is conducted with an expected resolution and/or course of action. U.S. Bank's Security Awareness For Everyone (SAFE) Program establishes U.S. Bank's enterprise information security awareness program to provide guidance for the protection of U.S. Bank business information, systems and processes to U.S. Bank employees, independent contractors and employees of temporary staffing agencies in support of U.S. Bank's Information Security Program. The required courses include specific courses based on an employee's role and access to systems. The training is refreshed annually. Upon completion of the SAFE courses, employees should be able to understand the U.S. Bank information classifications and how to handle information in each classification. No training from GSA is given to US Bank. US Bank reviews GSA rules and Regulations as it pertains to their Offer to GSA.

9.0 Accountability and Auditing

<p>PIA-9.1:</p>	<p>How does the system owner ensure that the information is used only according to the stated practices in this PIA?</p>	<p>U.S. Bank's Information Security Program undergoes annual audits performed by internal auditors, Corporate Audit Services. U.S. Bank's Information Security Program is regularly reviewed by independent auditors and assessors, both internal and external, and federal regulators. A formal report and information security strategy are presented to the U.S. Bank Board of Directors on an annual basis. Quarterly updates are also provided to the Board regarding progress toward strategic goals and other updates. Monthly metrics are communicated to senior management reflecting key performance indicators of the Information Security Program. If U.S. Bank business lines have privacy requirements over and above stated corporate policy, the business line ensures communication and compliance. All U.S. Bank personnel with access to GSA SmartPay PII undergo federal adjudication to moderate. 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. To ensure U.S. Bank employees, contractors and associates understand and carry out their Information Security Program roles and responsibilities, and are suitable for the roles they are considered for, security responsibilities are addressed in job descriptions, terms and conditions of employment and required training. All U.S. Bank employees, contractors and associates are trained on their applicable information security responsibilities and required to attest to their commitment to carry out their information security roles and responsibilities. New U.S. Bank employee orientation addresses information security topics. The onboarding and orientation process is managed by the Human Resources department. U.S. Bank's Security Awareness For Everyone ("SAFE") Program establishes U.S. Bank's enterprise information security awareness program to provide guidance for the protection of U.S. Bank business information, systems and processes to U.S. Bank employees, independent contractors and employees of temporary staffing agencies in support of U.S. Bank's Information Security Program. The required courses include specific courses based on an employee's role and access to systems. The training is refreshed annually. Upon completion of the SAFE courses, employees should be able to understand the U.S. Bank information classifications and how to handle information in each classification. GSA contract requires U.S. Bank to provide Information Security Awareness and Training records annually.</p>
-----------------	--------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------