



GSA SmartPay® - US Bank

Privacy Impact Assessment (PIA)

14 September 2020

POINT of CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Arpan Patel

Name of Program Manager/System Owner:

- David J. Shea

Signature Page

Signed:

DocuSigned by:
Arpan Patel
9B060AABDAF4477...
Information System Security Manager (ISSM)

DocuSigned by:
David Shea
04FDC8A45A964CA...
Program Manager/System Owner

DocuSigned by:
Richard Spidel
171D5411183F40A...
Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

| Date | Description | Version of Template |
|------------|---|---------------------|
| 01/01/2018 | Initial Draft of PIA Update | 1.0 |
| 04/23/2018 | Added questions about third-party services and robotics process automation (RPA) | 2.0 |
| 6/26/2018 | New question added to Section 1 regarding Information Collection Requests | 2.1 |
| 8/29/2018 | Updated prompts for questions 1.3, 2.1 and 3.4. | 2.2 |
| 11/5/2018 | Removed Richard's email address | 2.3 |
| 11/28/2018 | Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov | 2.4 |
| 4/15/2019 | Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208) | 2.5 |
| 9/18/2019 | Streamlined question set | 3.0 |
| 2/20/2020 | Removed email field from signature page | 3.1 |

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
- 1.2 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 1.3 Has an 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.
- 1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

SECTION 2.0 OPENNESS AND TRANSPARENCY

- 2.1 Will individuals be given notice before to the collection, maintenance, use or dissemination and/or sharing of personal information about them? If not, please explain.

SECTION 3.0 DATA MINIMIZATION

- 3.1 Why is the collection and use of the PII necessary to the project or system?
- 3.2 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.3 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.4 Will the system monitor members of the public, GSA employees, or contractors?
- 3.5 What kinds of report(s) can be produced on individuals?
- 3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

SECTION 4.0 LIMITS ON USES AND SHARING OF 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, maintenance, use, or dissemination?
- 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?
- 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 GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

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 (SSP) for the information system(s) supporting the project?
- 6.3 How will the system be secured from a physical, technical, and managerial perspective?
- 6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

- 7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

- 9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about GSA’s use of GSA SmartPay – US Bank (a.k.a. GSA SmartPay3 – US Bank or U.S. Bank Access Online, Voyager Fleet Commander Online, and Syncada). To accomplish its mission GSA Center for Charge Card Management must, in the course of GSA SMARTPAY-US Bank, 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]

A. System, Application, or Project Name:

GSA SmartPay – US Bank, as supported by U.S. Bank Access Online, Voyager Fleet Commander Online systems.

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. 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. 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

CPS (Corporate Payment Systems) develops and markets client-centric corporate payment solutions designed for medium and large sized companies or organizations, and State and Federal Government organizations (collectively referred to hereafter as “Clients”). CPS also provides unique services to Federal Government Agencies which are specifically highlighted in this report. CPS provides payment solutions that enable the exchange of value between buyers and sellers. CPS programs are designed to help improve expense management and streamline steps in the procurement process.

The following three applications that make up the GSA SmartPay - US Bank System:

Access Online

Access Online is a web-enabled program management and reporting tool offering a feature-rich platform that can be easily configured and deployed to meet the unique needs of clients. Clients have the flexibility to implement the features and functionality that best support and enhance their business processes. There are over one million active cardholder accounts for Access Online. Access Online has been developed based on the clients’ requirements. The four functional cornerstones of Access Online are:

- Streamline payment and procurement processes
- Convenient access to information, round-the-clock
- Complete integration with client financial systems
- Effective and efficient management controls

Voyager Fleet Commander Online

The Voyager Fleet Commander Online / Over The Road (OCR) System offers extensive fleet solutions for client fuel and maintenance needs. The Voyager Fleet Card is the fastest growing universal fuel and maintenance fleet card in the industry with regional, national, local and independent locations in all 50 states. The program is designed around the need for a single source provider for all card issuance, billing, payment and customer service. Voyager fleet accounts can be established by vehicle or individual cardholder name.

Syncada

Syncada is a global, cardless, internet-accessed, business-to-business (B2B) multibank invoice processing, financing and payment solution providing comprehensive payment process automation and settlement services to commercial and government buyers and sellers.

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 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

1.2 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?

Data is retrieved by Card or Account number, employee ID (if provided by the agency), and the name. GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program and GSA/GOV-3 Travel Charge Card Program SORNs apply to the information being collected.

1.3 Has an 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.

Not applicable. An ICR has not been submitted to or approved by OMB.

1.4 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 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'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.

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

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 clients' 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 – 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.

SECTION 3.0 DATA MINIMIZATION

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

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.

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

No. The System does not aggregate data on an individual. Program performance reporting can be aggregated; however it is by product (purchase, travel, fleet) and not by individual.

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.

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

N/A, from a system perspective, the systems do not monitor any users differently from other users.

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/OPC's 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.

3.6 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?

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).

SECTION 4.0 LIMITS ON USING AND SHARING 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?

Yes, the information in the system, application or project is limited to only the information needed to carry out the Government purpose of the collection. The collection is done based on Government needs for the card program functions and reporting needs.

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?

No. For example, GSA will not generate reports from Access Online and provide those to customer agencies as part of its shared service functionality.

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)?

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.

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

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.

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, 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/OPC's, 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/OPC's. 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.

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?

- 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 – U.S. Bank personnel

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.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes. ATO dated January 14, 2020

EXPIRATION DATE: March 15, 2022

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).

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

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 do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

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

7.2 What procedures allow individuals to access their information?

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.

7.3 Can individuals amend information about themselves? If so, how?

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.

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.

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.

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 owner ensure that the information is used only according to the stated practices in this PIA?

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.

^[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.