

# U.S. Department of Commerce

## Office of the Secretary



### Privacy Impact Assessment for the Department-Wide Use of General Services Administration (GSA) SmartPay 3 (Citibank Commercial Cards System)

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer  
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

09/30/2020

---

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

# U.S. Department of Commerce Privacy Impact Assessment

## Department-Wide Use of General Services Administration (GSA) SmartPay 3 (Citibank Commercial Cards System)

### Unique Project Identifier:

#### Introduction: System Description

*Provide a description of the system that addresses the following elements:*

*The response must be written in plain language and be as comprehensive as necessary to describe the system.*

Established in 1998, the General Services Administration's (GSA) SmartPay Program is the world's largest government charge card and commercial payment solutions program, providing services to more than 560 Federal agencies, organizations, and Native American tribal governments. GSA SmartPay payment solutions enable authorized government employees to make purchases on behalf of the Federal Government in support of their agency's mission. Currently, the Department of Commerce ("DOC" or "the Department") participates in GSA's SmartPay 3 initiative.

Under SmartPay 3 agencies issued task orders under the GSA SmartPay master contract and awarded their program to one of the GSA SmartPay contractor banks (Citibank or U.S. Bank). The banks then provide payment solutions to the agency employees to make purchases on behalf of their agency. You can read more about the GSA SmartPay program and SmartPay 3 specifically, at <https://smartpay.gsa.gov/>.

The GSA SmartPay Program offers four business lines of payment solutions: Purchase, Travel, Fleet, and Integrated. Table 1 describes each in more detail.

TABLE 1

Business Line	Description
Purchase	Purchase accounts are the preferred contracting and payment mechanism for micro-purchases of supplies and services in accordance with the Federal Acquisition Regulations. These accounts are generally used for things such as office supplies, training fees and registrations, and other similar goods and services.
Travel	Travel accounts may be used by individual government travelers to pay for all official Government travel and related expenses.
Fleet	Fleet accounts may be used for purchasing fuel and maintenance services for government vehicles. Fleet accounts are generally assigned to a vehicle, rather than an individual.
Integrated	Integrated accounts are combination of two or more business lines on a single account (for example, purchase and travel).

This PIA focuses on the purchase and travel business lines specifically, as these lines are used by DOC, are directly tied to an individual, and implicate the collection and processing of Personally

Identifiable Information (PII). GSA has documented the SmartPay 3 program in a PIA for each of the participating banks, including Citibank<sup>1</sup>.

To obtain a purchase account, an employee must be recommended by his/her supervisor, who then submits an application on his/her behalf through the program coordinator<sup>2</sup>. Potential purchase account holders must complete purchase cardholder training before being issued a card and using the purchase account.

For travel cards, all DOC employees are eligible to be issued a travel card. Employees are required to use an official travel charge card for expenses (excluding airline tickets) if they travel five (5) or more times in a year, unless they fall into an exempt classification. As such, employees are required to self-identify as requiring a travel account and apply accordingly. Additional information on the application and approval process for both purchase and travel cards is outlined below in Section d.

### **DOC's Use of SmartPay 3**

DOC selected Citibank as its contractor bank for providing payment services under SmartPay 3. As DOC's selected vendor, Citibank is responsible for establishing accounts for DOC employees authorized to make purchases on behalf of the Department. Additionally, Citibank is responsible for providing certain technical solutions to assist DOC in reconciling charges and submitting payment for each account, as well as data analytics capabilities to help meet agency reporting needs, improve security, and identify fraud, misuse, and abuse. This includes the development and transfer of regular reports to DOC for use by each of the individual Bureaus and Operating Units (OU). Citibank also provided support in transitioning from SmartPay 2 to SmartPay 3, by providing program forms (account applications, etc.), development, production, and delivery of new charge cards ("cards"), account activation, and training materials for account holders and designated officials within the agency with responsibilities related to financial accounting or reconciliation of purchases and payments.

Finally, Citibank hosts and makes available to DOC, an "Electronic Access System" or "EAS", in which authorized DOC users use to review accounts and perform functions related to account reconciliation, or, in the case of account holders, to manage their account – this includes 24/7 online support through CitiManager, as well as a customer service phone numbers for cardholders (e.g. balance, suspected fraud or misuse, lost card, etc.).

There are two types of accounts within the GSA SmartPay Program. Centrally billed accounts (CBAs) are directly billed to and paid for by an agency. Individually billed accounts (IBAs) are directly billed to and paid for by individual agency account holders (e.g. employees). At the DOC, there are both CBA and IBA travel accounts, while purchase card accounts are always CBAs.

---

<sup>1</sup> The GSA SmartPay3 Citibank PIA is available at <https://www.gsa.gov/reference/gsa-privacy-program/privacy-impactassessments-pia>.

<sup>2</sup> This process is described in greater detail in the Commerce Acquisition Manual (CAM), 1313.301 – Purchase Card Program, available at [http://www.osec.doc.gov/oam/acquisition\\_management/policy/commerce\\_acquisition\\_manual\\_cam/](http://www.osec.doc.gov/oam/acquisition_management/policy/commerce_acquisition_manual_cam/).

*(a) Whether it is a general support system, major application, or other type of system*

SmartPay 3 involves a series of systems across DOC and Citibank networks. Section d. below describes each of these systems in greater detail.

*(b) System location*

Citibank's system is primarily located in New York, New York, while the Department's system(s) are in two primary locations: National Oceanic and Atmospheric Administration (NOAA) Information Technology Center (ITC) in Landover, Maryland, and the Herbert C. Hoover Building (HCHB) in Washington, DC.

*(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

To receive daily downloads from Citibank and to provide uploads for payment reconciliation, the Department, through NOAA, has entered into an Interconnection Security Agreement (ISA) for the NOAA ITC to connect to Citibank's General Support System (GSS). The purpose of the exchange of data between Citibank and NOAA's ITC is to support the daily transfer of purchase and travel account data, as well as monthly invoice and correction files for distribution to the various Bureaus within the Department. Citibank daily file transfers to the NOAA ITC will be used by the National Institute of Standards and Technology (NIST) to feed into the NIST MyTools application for solvency analysis and Budget Solvency Tool (BST) Obligation in Process analysis. A Master Information Sharing Agreement (ISA) governs the entirety of all connections between Citibank systems and DOC systems, as well as any internal connections between DOC Bureau systems. NOAA ITC shares a secure interconnection with the Bureau of Census (CEN04-CBS) and NIST (CEN/CBS 162-01). Additional details of this connection and data sharing is outlined in the PIA for the NOAA ITC<sup>3</sup>.

*(d) The way the system operates to achieve the purpose(s) identified in Section 4*

SmartPay is made up of five operational components:

- **Citibank GSS:** Maintains account information for DOC travel and purchase accounts, including all identifying information associated with the account, purchases, balances, limits, restrictions, account codes, and other account and transaction related information.
- **Citibank EAS:** A Citibank owned and operated Major Application which provides access for limited DOC personnel to review, manage, create, or close DOC accounts and for account/card holders to manage their accounts. The Citibank EAS includes the "CitiManager" solution – a web and mobile based application which allows for access by Cardholders, Approving Officials, and Agency Program coordinators to access and manage DOC accounts. While CitiManager is available through a mobile application, access is limited to Cardholders only – and only for basic card management functions, such as viewing transactions, statements and payments.

---

<sup>3</sup> The NOAA ITC is addressed under the Privacy Impact Assessment for NOAA 1101, available at [http://www.osec.doc.gov/opog/privacy/NOAA%20PIAs/NOAA1101\\_PIA\\_SAOP\\_Approved.pdf](http://www.osec.doc.gov/opog/privacy/NOAA%20PIAs/NOAA1101_PIA_SAOP_Approved.pdf) .4

Approving Officials and Agency Program Coordinators cannot access the EAS via a mobile application, and Cardholders can't make any account changes via the mobile application.

- **Use Monitoring Capabilities:** Compliance and reporting tools that systematically identify transactions for Program Administrators which may implicate misuse, abuse, or fraud, as well as opportunities for gaining insight into agency purchasing habits and practices.
  - **Visa Intellilink:** A cloud-based information and expense management solution which allows administrators and cardholders to effectively manage spending, implement control through automated workflows, and gain spend insights through a suite of tailored reporting.
- **Citibank EAS Transaction Management:** Transaction Management is a module within Citibank's EAS which provides access for limited DOC personnel to reconcile and approve purchase card transactions and the recording of financial, procurement, and property information. Transaction management is a web-based application that provides certain DOC employees (those designated as "Approving Officials" or "AO") access to financial transactions against DOC purchase accounts using electronic bankcard statements which eliminate paper-based processing and reporting. Transaction data is available in Transaction Management after transactions are posted by merchants. AOs are responsible for bankcard activity for their cardholders (by Bureau or OU). AOs review bankcard transactions and approve the transactions. Transaction Management provides an automated approval process which allows AOs to drill down to details for each transaction.
- **DOC Bureau and OU Local network file shares, databases, and secure locations:** GSS and MA's which are used by the various Bureaus and OUs to download, house, and review files and reports generated by Citibank's EAS and house applications and supporting documentation for travel and purchase card accounts.

These five components support the following primary daily operations associated with the program:

- Request for, creation and distribution of purchase cards, and use of said cards by authorized DOC employees in support of mission-related needs.
- Management and reporting on Citibank provided card programs by select DOC employees through the Citibank EAS;
- Monitoring use of cards by authorized DOC employees for misuse, fraud, waste and abuse, as well as for opportunities for improvement(s) in the program;
- Daily and monthly reporting to include secure transfer of purchase, travel and fleet card data between DOC and Citibank; and
- Secure retrieval of daily and monthly purchase card data files from NOAA by the participating Bureaus within the DOC.

A general description of the overall system lifecycle is captured in Figure 1 below.

FIGURE 1



## **Account Creation and Card Issuance**

### **Existing Account Holders**

DOC account holders (both travel and purchase) under GSA SmartPay 2 were issued new cards for use in April 2019. Information associated with accounts under SmartPay 2 was transferred to Citibank by the DOC, resulting in a seamless experience for existing DOC account holders. No new information was collected from existing account holders.

Information, including PII, such as names, account numbers, Social Security number (SSN)<sup>4</sup>, date of birth (DOB) and other identifying information associated with an account was transferred via secure file transfer from DOC to Citibank. Travel account holders continued to receive statements at the address they had previously provided. Account holders for travel and purchase continued to use their new cards just as they did their old cards. Existing travel account holders were not be subject to re-application or new credit worthiness checks. All existing account holders were required to activate their cards upon receipt using Citibank's online activation mechanism or by telephone. Travel card holders used the last four digits of their SSN to activate, whereas Purchase Card holders were issued a specific activation code which is generated by DOC. These users then select a PIN to associate with their card and may self-register the card for account access and management via the CitiManager solution.

### **New Account Holders**

<sup>4</sup> Applies to Travel Card holders only.

For new account holders, DOC established a process for requesting and receiving approval for an account and establishing an account through Citibank. All new account holders – both travel and purchase – must complete training outlining their roles and responsibilities as account holders and certify, in writing, they have read and understood all relevant policies, procedures, and rules regarding use of their DOC-issued account(s).

### ***New Travel Accounts***

New account holders for travel accounts are required to complete an application for an account with Citibank and to review and consent to the cardholder agreement. Applications may be submitted electronically, via Citibank’s online application, or by paper form. When applying, DOC employees must provide the following PII:

- Full name (first, last, middle initial)
- Name as it will appear on card
- Social Security number (SSN)<sup>5</sup>
- Date of Birth (DOB) as MM/DD/YYYY<sup>6</sup>
- An address to associate with the card (for statement delivery). This may be a home or work address and includes Street, City, State, ZIP code, and country
- Business telephone number

Individuals are provided a Privacy Act Statement (e3) as part of the collective notice and terms and conditions of application on the application. Individuals must provide all requested information when applying for a new travel account – incomplete applications will be rejected.

Citibank’s internal process requires that, after assessment by Citibank, DOC’s agency program coordinator approves the request for a new account prior to issuance of the card. In approving requests, DOC agency program coordinators are not provided PII beyond basic contact information of the applicant and whether the account has any restrictions. New account holders are subject to a credit-worthiness check, conducted by Citibank, in accordance with rules outlined in guidance from the Office of Management and Budget (OMB).<sup>7</sup>

This credit check is used only to determine if a card will be issued and, if so, whether the issued card will be subject to a credit limit restriction. In general, scores over 660 are not subject to a credit limit restriction, while scores between 500 and 660 are subject to a restriction – specifically a reduced credit limit amount. Scores under 500 may be denied a card. In the case of a denial, an employee will have the option of requesting a travel advance or using personal funds upfront and requesting reimbursement through the voucher process. Credit checks are considered “soft hits” on an employee applicant credit file, generally do not negatively impact credit score, and drop off after a period. Employee applicants may refuse this credit check, but, if they do, are, by default, issued a restricted card. DOC, including individuals who manage the travel card program, are not provided the results of these credit checks (e.g. credit scores), only whether a restriction was placed on a specific card because of the check.

---

<sup>5</sup> Applies to Travel Card holders only.

<sup>6</sup> Applies to Travel Card holders only.

<sup>7</sup> See OMB Circular 123-A, Appendix B.

Upon submission, and approval, approved applicants will be issued a card for their travel account and may begin using the card in accordance with DOC and Federal rules, regulations, and policies related to travel card usage. Cardholders are required to “activate” their card with a specific variation code that only they know – the last four digits of their SSN. Cardholders may also choose to register for online access to the account management tool. As part of training and awareness efforts, the Department has put together various training opportunities, guides, and learning aids for DOC employees who hold travel cards, regarding how to activate their card and manage their card through the online capability.

### ***New Purchase Accounts***

New account holders for purchase accounts must be nominated, in accordance with DOC policy<sup>8</sup>, by their supervisor, through the agency program coordinator via a written justification for issuance of a purchase card. Individuals are provided notice of the collection and use of their information by their supervisor at the time of nomination by the supervisor. This nomination package should also include a copy of the proposed account holders applicable training certificates and proposed single purchase and monthly spending limits. Upon approval of a cardholder’s nomination package and issuance, the agency program coordinator will order a purchase card (for cardholders only), enter account profile data into Citibank’s tool and provide user access information and guidance. Upon receipt of the card, users activate the card via Citibank’s online tool or the phone using the provided four-digit code, choose and set the PIN associated with the card, and, if they choose, register the card and account for online management and access through the CitiManager tool.

### **Purchase, Use, and Management**

Account holders may use their Citibank-issued DOC purchase and travel cards for select, approved goods and services as it relates to their official duties and in accordance with Federal and DOC rules, regulations, and policies. DOC employees use their cards like any regular credit card, by presenting the card at the point of sale for an approved transaction.

As noted above, purchase cards at DOC are CBAs, while travel cards are IBAs and CBAs. IBAs are directly billed to and paid for by individual agency account holders – employees receive a monthly statement at the address they provided at the time of application for an account, and are responsible for making payment, in full, by the payment due date presented on the statement. For CBAs, account holders are responsible for reviewing their statements and alerting their agency program coordinator of any discrepancies or unauthorized purchases to facilitate reconciliation. Designated officials within DOC are then responsible for remitting payment directly to Citibank on behalf of all DOC purchase and travel CBA account holders.

---

<sup>8</sup> See CAM 1313.301

## Reconciliation

Accurate record keeping is critical to the success of the government purchase card program and ensures that any improper, incorrect or fraudulent charges, or duplicate payments are addressed in a timely manner. DOC Account Holders and AOs use a combination of manual and automated reconciliation procedures, depending upon whether the account is an IBA or a CBA.

### *Reconciling Purchase CBAs*

For purchase CBAs, accounts are reconciled monthly. Account holders are responsible for reviewing the itemized statement and comparing each transaction listed on the purchase card ordering log with the statement to ensure accuracy. Additionally, account holders are responsible for checking that the appropriate accounting codes are assigned to each transaction. After reviewing the statement and compiling the necessary reconciliation documents, account holders submit the reconciled statement to their AO for approval. Reconciliation documentation include:

- Purchase card ordering log
- Statement of account,
- Reconciled transactions
- Supporting documentation

Account holders are responsible for maintaining an electronic or hard copy of the reconciliation package sent to the AO for review and approval.

Upon receipt of the reconciled statement and supporting documentation, AOs review the reconciliation material to ensure that all required documentation has been submitted; and all items purchased are for official Government use and comply with applicable laws, regulations, policies, and guidance. Upon verification and approval, AOs retain reconciliation files for six years from final payment of transactions. Citibank's EAS tools retains all transaction data for the six-year retention period.

Any disputes over specific charges by the account holder are to be managed via Citibank's dispute process and in accordance with DOC procedures for managing disputed transactions as outlined in the Commerce Acquisition Manual 1313.301 – Purchase Card Program.

Account holders and AOs ensure that purchases made with the purchase card are in accordance with all Federal, DOC and Bureau or OU laws, regulations, policies and guidance. Cardholders and approving officials may be held personally liable for any action deemed by the reviewing official as noncompliant with laws, policies and regulations. In addition, if it is determined the transactions are made with the intent to commit fraud or constitute waste or abuse, the cardholder and approving official may face disciplinary actions under Department Administrative Order (DAO) 202-751, Discipline, and applicable Government-wide administrative procedures, including suspension and termination of employment.

### *Reconciling IBAs*

As noted above, IBAs are directly billed to and paid for by individual agency account holders; employees receive a monthly statement at the address they provided at the time of application for

an account, and are responsible for making payment, in full, by the payment due date presented on the statement. Travel account holders are responsible for ensuring that the address on file for receiving statements remains current – accounts that have statements returned to Citibank due to a bad address will be closed. IBA travel account holders are to pay their travel card account, in full, upon receipt of the account statement, but no later than 30 calendar days from the closing date on the statement in which the charge(s) appeared. Cardholders may use the CitiManager solution or pay their card by U.S. mail or phone. In remitting payment, additional PII may be necessary, including name, contact information, and banking account information – such as an account number and routing number – to facilitate an electronic funds transfer (EFT).

To facilitate reimbursement by DOC, employees are required to submit travel vouchers to their servicing finance office within five working days after the completion of travel, or every 30 days if on an extended tour-of-duty. Timely voucher submission is critical since employees are personally responsible for paying their travel card bills on time, regardless of whether they have been reimbursed for their vouchers.

Travel card accounts that may be subject to late fees – the first late fee will be assessed at day 75 (two billing cycles plus 15 days) and the second late fee will be assessed at 90 days past due, with monthly fees thereafter. In general, late fees incurred for non-payment are the responsibility of the account holder, however, if the government is responsible for the delay in payment, late fees are reimbursable. Accounts which are 61 – 120 days past due will be suspended until payment is made, while travel card accounts that are 121 days or more past due will be cancelled. At this point, account holders may be eligible for enrollment in salary offset or similar methods to recover the debt.

Citibank does not report cardholders to the credit bureau unless and until they charge off – 210 days past due, and a salary offset procedure will likely be utilized before charging off an account. Cancelled accounts paid through salary offset will not be reported to the credit bureaus. Simply having a government travel card does not generally impact an employee's credit rating. In general, travel card issuing banks generally do not report travel card activity to the credit bureaus unless the account charges off, and accounts which are well managed will not increase a cardholder's credit score.

As with purchase accounts, travel card account holders are responsible for handling any disputes over specific charges with Citibank directly, via Citibank's processes. Failure to report disputed charges within 90 days from the date of the transaction may result in the account holder being liable for the disputed charge. Procedures specific to disputes and requirements of travel account holders is outlined in the Department of Commerce's Travel Card Handbook.

All rights and privileges afforded under the Fair Credit Reporting Act (FCRA)<sup>9</sup> apply to travel cardholders, and free credit bureau reports (as mandated by the FCRA) are available (1 per year per bureau) by visiting the FTC's [annualcreditreport.com](http://annualcreditreport.com) website.

When applying for a travel account, employees must review and agree to the cardholder agreement, which stipulates that cardholders are “responsible for all purchases, cash advances, and fees charged to the card issued to me...” and that “the Bank will seek payment for all

charges directly from me regardless of whether I have been reimbursed by the DOC.” Additionally, there is no condition on payment after reimbursement. As with purchase card accounts, travel account holders are subject to disciplinary action if found in violation of or noncompliant with laws, policies and regulations in their use of the travel card.

## **Reporting and Analysis**

Certain DOC employees with duties related to financial management and oversight have access to the Citibank provided EAS, which allows these employees access to information about individual accounts, including current and outstanding balances, purchase and transaction history, payment history, and other information necessary for managing DOC accounts and ensuring that they remain in good standing. Additionally, Citibank’s EAS has reports of all transactions and payments, as well as other information, about DOC accounts.

In the EAS, certain sensitive PII fields have been masked, truncated, or otherwise made unavailable for viewing by end-users. These fields are not essential for the duties associated with access to the reports and generally include SSN, DOB, and account number.

## **Account Closure**

Generally, a change in an account holder’s status – transfer, retirement, resignation or termination – necessitates closure of a travel or purchase card account. Employees undergoing a change in status are required to stop using their account in advance of their separation date, if possible, to allow outstanding transactions to be processed and reconciled before their separation.

Additionally, account holders are required to destroy their purchase and/or travel card by cutting it in half and providing the destroyed card to their agency program coordinator or AO, per Bureau or OU policy; advise the AO of any outstanding transactions; provide the AO with any remaining receipts or other documents related to outstanding transactions; and follow standard Bureau or OU checkout procedures.

Account holders who fail to comply with these procedures may have their separation delayed. AOs are responsible for determining when to close the account based on the outstanding transactions and for notifying the agency program coordinator of the need to close the account. The agency program coordinator is responsible for closing the card account when it becomes apparent that a cardholder has separated from DOC, or their status has changed.

### ***(e) How information in the system is retrieved by the user***

In general, retrieval of information across the system is by account number or account holder name. More specifically: Account holders may retrieve limited information about their account by contacting the customer contact center provided by Citibank (number is located on the back of their card) and providing their account number and other, limited identifying information (for identity verification and security purposes). Purchase account holders also may retrieve limited information about their account in the form of a statement by logging in and reviewing their

statement (as required) during monthly reconciliation – statements are generated by a date range and reconciliation status.

Agency program coordinators and other DOC employees with duties related to financial management and account reconciliation, may retrieve information about a specific account by account number or name associated with the account. Certain privileged users may also be able to retrieve account information in the EAS by the SSN associated with a specific account.

*(e) How information in the system is retrieved by the user*

In general, retrieval of information across the system is by account number or account holder name. More specifically:

Account holders may retrieve limited information about their account by contacting the customer contact center provided by Citibank (number is located on the back of their card) and providing their account number and other, limited identifying information (for identity verification and security purposes). Purchase account holders also may retrieve limited information about their account in the form of a statement by logging in and reviewing their statement (as required) during monthly reconciliation – statements are generated by a date range and reconciliation status.

Agency program coordinators and other DOC employees with duties related to financial management and account reconciliation, may retrieve information about a specific account by account number or name associated with the account. Certain privileged users may also be able to retrieve account information in the EAS by the SSN associated with a specific account.

*(f) How information is transmitted to and from the system*

Information about existing SmartPay 2 account holders who would also be account holders under SmartPay 3 was transmitted via secure file transfer protocol (SFTP) from DOC to Citibank.

Information about new travel account holders is transmitted via an electronic application, completed by the employee applicant, and submitted directly to Citibank via a secure web interface. In the case of paper applications, transmittal will occur through secure email. As outlined above, all DOC employees are eligible to apply for and receive a travel card, however, employees are required to use an official travel charge card for expenses (excluding airline tickets) if they travel five (5) or more times in a year, unless they fall into an exempt classification. . Prior to applying online, employees must complete the Travel Charge Card Training course available from GSA and provide a copy of the completion certificate to their supervisor, AO, and Agency Organization Program Coordinator (AOPC). Applications are subject to review and approval by the Supervisor and AO, the AOPC in accordance with the procedures and requirements outlined in the Department of Commerce's Travel Card Handbook.

Upon approval by the Supervisor, AO, and AOPC, the application is processed by Citibank, who will process the application and conduct a credit worthiness check of the applicant as discussed above.

Information about new purchase account holders is provided by form to agency program coordinators and then directly input by authorized employees within DOC with access to the Citibank EAS. As outlined above, OU and Bureau officials are responsible for nominating prospective purchase account holders and providing those nominations to the agency program coordinator with a written justification for issuance of a purchase card along with the applicable training certificates and proposed single purchase and monthly spending limits.

*(g) Any information sharing conducted by the system*

Information sharing is limited to sharing between DOC (NOAA ITC) and Citibank (GSS) systems for the purposes of account management and reconciliation, and internally between DOC bureaus (as outlined in Section c. above and in accordance with the Master ISA) and across DOC financial management systems for the purposes of payment, reconciliation, and reporting suspected or confirmed fraud, waste, and abuse. Information may be shared internally with the Office of Financial Management (OFM) Data Analytics Program in support of identifying systemic issues related to fraud and abuse. The OFM Data Analytics Program discusses collection and use of this information in more detail. Other internal DOC systems with which information is shared are covered by their own separate PIA.

*(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

E.O. 9397; E.O. 12931; 40 U.S.C. Sec. 501-502; 5 U.S.C. 5707 and as implemented by the Federal Travel Regulation (FTR), 41 CFR 300-304; E.O. 9397, as amended; E.O. 11609, as

*(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Moderate

**Section 1: Status of the Information System**

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.  
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)				
a. Conversions		d. Significant Merging		g. New Interagency Uses
b. Anonymous to Non-		e. New Public Access		h. Internal Flow or

Anonymous				Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

— This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

— This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

## **Section 2: Information in the System**

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (*Check all that apply.*)

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card	X	m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					

\*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

The social security number is required for travel account holders because travel account holders are subject to a credit-worthiness check in accordance with rules outlined in guidance from the Office of Management and Budget (OMB). This credit check is used only to determine if a card will be issued and, if so, whether the issued card will be subject to a credit limit restriction.

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

<b>Work-Related Data (WRD)</b>					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>					

2.2 Indicate sources of the PII/BII in the system. (*Check all that apply.*)

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone		Email			
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

<b>Non-government Sources</b>					
Public Organizations		Private Sector	X	Commercial Data Brokers	X
Third Party Website or Application					
Other (specify):					

## 2.3 Describe how the accuracy of the information in the system is ensured.

DOC and Citibank have internal checks for verifying the accuracy, timeliness and completeness of data within their own systems. Reports are also produced that have number of accounts and amounts for data transmissions.

DOC account holders provide their information when applying directly through Citibank for a travel card or in being recommended for a purchase card. Additionally, statements must be reviewed for accuracy by account holders and Program Administrators monthly. As noted above, for travel account holders, cardholders are responsible for ensuring that the address on file and associated with the account is accurate – accounts that have statements returned to Citibank due to a bad address will be closed.

Regarding data transferred from Citibank to DOC (NOAA) for daily and monthly transactions – there are a series of checks and edits that the CBS Centers performs to ensure that all the data elements are in place in any incoming data. It also reconciles the number of records and amount that were staged to process through with the number and amount processed to ensure there is a match. Data is encrypted at both the transport and file layers to ensure integrity.

## 2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (*Check all that apply.*)

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</b>		
Smart Cards		Biometrics
Caller-ID		Personal Identity Verification (PIV) Cards
Other (specify):		

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

**Section 3: System Supported Activities**3.1 Indicate IT system supported activities which raise privacy risks/concerns. (*Check all that apply.*)

<b>Activities</b>			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	X
Other (specify):			

There are not any IT system supported activities which raise privacy risks/concerns.
--

## **Section 4: Purpose of the System**

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.  
*(Check all that apply.)*

<b>Purpose</b>			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session )		For web measurement and customization technologies (multi-session )	
Other (specify):			

## **Section 5: Use of the Information**

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII about DOC employees who are prospective or current account holders includes:
• Full name (first, last, middle initial)
• Name as it will appear on card
• Social Security Number (SSN)
• Date of Birth (DOB) as MM/DD/YYYY
• An address to associate with the card (for statement delivery). This may be a home or work address and includes Street, City, State, ZIP code, and country
• Telephone Number (business or personal)
• Email address (business or personal)
• Transactional information associated with the account
• Payments, balances, limits, and restrictions (based on credit worthiness evaluation) associated with the account

PII about DOC employees who serve as Approving Officials or whose duties related to financial management include access to the EAS or other internal DOC systems which process PII associated with this system includes:

- Name
- Business email address
- Username(s) and password(s)

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

*There is a risk associated with the collection and use of sensitive PII in the request, approval, establishment, and maintenance of accounts:* Information collected and processed in support of the SmartPay 3 program is limited to that which is necessary for identifying prospective account holders, including identifying a specific individual applicant; evaluating and approving requests for accounts, including determining credit worthiness to set credit limits; creating and maintaining travel and purchase accounts through Citibank – including creating and distributing purchase and travel cards, making purchases, providing statements and reconciling charges and payments, and monitoring transactions for compliance with applicable Federal and DOC laws, policies, and guidelines; and reporting on purchase and travel account use to internal DOC stakeholders. DOC and Citibank, have taken steps to ensure that data collected and maintained in administration of the SmartPay 3 program is appropriately protected. DOC systems which collect or process data in support of the SmartPay program have controls in place to prevent the loss of confidentiality, integrity, or availability of PII, as well as prevent misuse of the data. DOC systems authorized to operate in accordance with the Federal Information Security Modernization Act (FISMA) and with OMB directives and NIST standards, to include the privacy and security controls outlined under NIST 800-53. Additionally, DOC has made additional business decisions to reduce the risk presented to PII, including not collecting or using Social Security numbers (SSNs) for purchase cards, masking certain sensitive data elements from view in the EAS, implementing multi-factor authentication, placing additional requirements on Citibank in the incident detection and reporting process, and outlining a set of conditions specific to the GSA ATO including regular status and progress updates on an identified set of controls for the system.

GSA as the shared services provider for the SmartPay 3 program is responsible for reviewing the security posture of the Citibank system, evaluating the associated risks, and providing an Authority to Operate (ATO) which can then be leveraged by customer agencies (such as DOC) under the BPA, in making their own risk acceptance determinations. Controls are defined in the GSA master contract and additional, supplemental requirements are outlined in the task order between Citibank and DOC. Section 8.2 includes an additional discussion of these controls and GSA's assessment of Citibank system(s). Additionally, DOC has documented via a Master ISA, the interconnection between DOC system(s) and Citibank

system(s), as well as connections between internal DOC systems at the various Bureaus to map data flow and outline controls implemented to protect PII at various points in the lifecycle across interconnected systems.

## **Section 6: Information Sharing and Access**

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus	X	X	X
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector		X	X
Foreign governments			
Foreign entities			
Other (specify):			

The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
	The system connects to NOAA's ITC via secure connection as outlined in the ISA between NOAA and Citibank. Transmission of data is encrypted at a FIPS 140-2 standard. Additionally, an ISA exists between the Office of the Secretary (OS) within DOC and the participating Bureaus for the internal exchange of data related to the purchase card program for the Department. Finally, for new applicants for travel cards, applications may be processed via manual form and sent to Citibank via secure email transmission.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

## **Section 7: Notice and Consent**

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:  For Travel Accounts, notice is provided via the Privacy Act Statement available on the travel card application. Additional notice is included in the cardholder agreement provided in the user application form/agreement.  For Purchase Card Accounts, notice is provided via this Privacy Impact Assessment and the applicable System of Records Notice (SORN) as referenced in Section 9.	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: Notice is also provided via training offered by Citibank, GSA, and DOC for prospective cardholders, as well as through this PIA and the PIA provided by GSA for the SP3 program.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals may choose to decline to provide information, however, doing so may result in denial of issuance of a travel card or a purchase card.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals may choose to decline to apply for a travel card or provide their PII for a purchase card, however, if they apply, they consent to provide all required information and to have such information used as necessary in maintaining their account. Individuals may decline to be subject to a credit worthiness check as part of their application for a travel card, however, if they refuse, they will be issued a restricted card.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to	Specify how: Individuals may make a request under the access provisions of the Privacy Act of 1974, As Amended.
-------------------------------------	---	---

	them.	Additionally, individuals may have access to information associated with their account via statements (either received directly for travel cards or provided for purchase cards) or by working directly with their Program Administrator or Citibank to access, review, and update certain information associated with their account. Please note, this may be limited. Some information, such as information used to detect fraud, misuse, or abuse, or transactional information, may not be available for review or update by account holders. Other information, such as billing address, contact information for Travel Card holders may be updated through the CitiManager online tool if the card and account were registered at time of receipt.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

## **Section 8: Administrative and Technological Controls**

**8.1** Indicate the administrative and technological controls for the system. (*Check all that apply.*)

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Both DOC and Citibank have implemented auditing capabilities for the various systems through which data in support of the SmartPay program flows.
<input checked="" type="checkbox"/>	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>GSA issued an extension of the existing ATO for the system effective August 14, 2020. The extension expires on February 13, 2021. Review of ATO resulted in determination that risk was acceptable for operation.</u> <input type="checkbox"/> <u>This is a new system. The A&amp;A date will be provided when the A&amp;A package is approved.</u>
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestone (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

**8.2** Provide a general description of the technologies used to protect PII/BII on the IT system. (*Include data encryption in transit and/or at rest, if applicable.*)

The General Services Administration (GSA) as the shared services provider for the SmartPay 3 program is responsible for reviewing the security posture of the Citibank system, evaluating the associated risks, and providing an Authority to Operate (ATO) which can then be leveraged by customer agencies (such as DOC) under the BPA, in making their own risk acceptance determinations. The most current ATO, which expired August 14, 2020 was conditionally extended and remains effective through February 13, 2021, was reviewed by the Department's Chief Information Officer and Chief Privacy Officer and the risk deemed acceptable for operation (and documented). Conditions for extension of operation and risk acceptance have been outlined.

GSA has authorized the Citibank system(s) at a Moderate level. All applicable controls (for a moderate baseline) outlined in the NIST 800-53, Rev 4 family of controls, including those privacy specific controls outlined in Appendix J were evaluated for implementation for the previous version of the program. GSA also developed a crosswalk to map Payment Card Industry (PCI) controls and requirements to those found in NIST 800-53 to ensure a fulsome evaluation of all available and applicable controls. Additional specifications for technical and administrative safeguards and minimum standards were outlined in the master contract between Citibank and GSA. Implementation of these safeguards was evaluated as part of GSA's overall assessment of the Citibank system. In general, these safeguards include:

- Encryption of PII in transit – PII is encrypted during transit between Citibank and the DOC (NOAA ITC). During transmission, data is encrypted at both the file and transport layer(s).
- All data is housed in the United States.
- Physical data centers are protected using appropriate entry controls to limit and monitor physical access to systems.
- Incident monitoring, detection, reporting, and response processes and procedures are in place, including additional requirements specific to detection of incidents involving loss or compromise of PII.
- Regular monitoring of system for security vulnerabilities and regularly scheduled patches.
- Continuous logging and monitoring of system and protection of logs. Use of up-to-date anti-virus software and performance of daily scans and generation of audit logs.
- Use of two-factor authentication.
- Certain sensitive data elements (SSN, DOB) are only collected for Travel Card holders and are not collected for Purchase Card holders. Additionally, these data fields, and other potentially sensitive data fields (such as card/account number) are masked, truncated, or otherwise obscured from view in the EAS by end users of that system.

## **Section 9: Privacy Act**

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

\_\_\_\_\_ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. (list all that apply): <a href="#">GSA/GOVT – 3 Travel Card Charge Program, April 3, 2013</a> <a href="#">GSA/GOVT – 6 GSA SmartPay Purchase Charge Card Program, April 25, 2008</a> <a href="#">COMMERCE/DEPT – 9 Travel Records (Domestic and Foreign) of Employees and Certain Other Persons</a> <a href="#">COMMERCE/DEPT – 18 Employee Personnel Files Not Covered by Notices of Other Agencies</a> <a href="#">COMMERCE/DEPT – 25 Access Control and Identity Management System</a>
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

## **Section 10: Retention of Information**

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. (Check all that apply.)

X	There is an approved record control schedule. Provide the name of the record control schedule:  <a href="#">General Records Schedule (GRS) 1.1 – Financial Management and Reporting Records</a>
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. (Check all that apply.)

<b>Disposal</b>			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

## **Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level**

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. (The PII

*(Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.  
*(Check all that apply.)*

X	Identifiability	Provide explanation: PII included in the system includes direct identifiers – such as full names, unique identifying numbers (SSNs, etc.), as well as date of birth. While some data is masked from view by end users, the combination of data included in the system presents unique opportunities to identify specific DOC employees.
X	Quantity of PII	Provide explanation: The system contains a moderate number of records (less than 10,000) - specifically, transactional records – related to purchase and travel accounts for DOC employees. While the total number of account holders is not especially large, the volume of information about each account increases overall sensitivity of the system.
X	Data Field Sensitivity	Provide explanation: Includes data that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. This includes both standalone data elements (such as SSN), as well as combinations of data such as name and credit card number. Additionally, data includes sensitive financial information (account numbers, transactions, payments, balance, credit worthiness, etc.) and limited positional data of DOC employees, including those in law enforcement or similar positions.
X	Context of Use	Provide explanation: Information is collected for, or used in the administration of benefits or privileges, or determining eligibility for such, or such information is otherwise used in making determinations about an individual.
X	Obligation to Protect Confidentiality	Provide explanation: Explicit promises of confidentiality regarding the information have been conveyed to the subject individual at the time or point of collection, and information is afforded confidentiality from unauthorized disclosure by statute or regulation (Privacy Act of 1974) and industry-specific (GLBA) obligations.
X	Access to and Location of PII	Provide explanation: PII is maintained or stored non-locally (e.g. a thirdparty location). Access limited to internal DOC employees and contractors with a bona-fide need-to-know the information.

	Other:	Provide explanation:

## **Section 12: Analysis**

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

*There is a risk of negative stigma associated with the evaluation of employees' credit worthiness in approving a travel card account.* As outlined above, new account holders are subject to a credit-worthiness check, conducted by Citibank, in accordance with rules outlined in guidance from OMB in Circular 123-A, Appendix B. This credit check is used only to determine if the issued card will be subject to a credit limit restriction on the card. Employee applicants may refuse this credit check, but, if they do, are, by default, issued a restricted card. DOC, including individuals who manage the travel card program, are not provided the results of these credit checks (e.g. credit scores), only whether a restriction was placed on a specific card because of the check. Only a limited set of DOC employees, including AOs and Program Administrators for the SmartPay program have access to this level of granular data about a specific user, account, or card, and only on a need-to-know basis. In general, an employee's supervisor or colleagues would not have access to this information or be aware of a credit limit imposed on a travel card assigned to that employee.

*There is a risk that individuals may not fully consent to the collection and use of their information or how their information is being used.* Travel and purchase card holders under SmartPay 3 are afforded several methods of notice related to their application for, use, and management of their account. Travel card applicants are provided notice in the form of a Privacy Act Statement at time of application, as well as supplemental privacy notice(s) in the cardholder agreement and the annual privacy policy notice provided by Citibank under the Graham-Leach Bliley Act. Purchase card applicants are provided notice at the point of application through the online application process. All account holders who use the CitiManager system receive notice, in the form of a privacy policy, at the bottom of the login page for the system. Finally, this PIA provides notice of the collection and use of this information in support of DOC's participation in SmartPay 3. By applying for a travel card, or requesting a purchase card, employees consent to the collection and use of their PII in creating and managing those accounts. Employees who apply for a travel card may decline a credit-worthiness check, however, if they decline such a check, they will be issued a restricted card.

*There is a risk that individuals may not fully understand how the application for or use of a government-issued travel or purchase card impacts their personal credit history.* In general, simply having a government travel card does not generally impact an employee's credit rating. Citibank does not report travel card activity to the credit bureaus unless the account charges off. Likewise, accounts which are well managed will not increase a cardholder's credit score. Credit checks for travel accounts are considered "soft hits" on an employee applicant credit file and do not impact overall score. Procedures specific to disputes and requirements of travel account holders is outlined in the Department of Commerce's Travel Card Handbook. All rights and privileges afforded under the FCRA apply to travel cardholders.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

<input checked="" type="checkbox"/>	<p>Yes, the conduct of this PIA results in required business process changes.</p> <p>Explanation: DOC worked with GSA and Citibank to update language in the existing Task Order agreement to clarify roles, responsibilities, timelines, and obligations associated with incident response, in the event of a breach of PII.</p> <p>DOC documented all information flows between Citibank systems(s) and DOC systems, including internal to the DOC Bureaus in a Master ISA.</p> <p>DOC updated the application/nomination process for Purchase Card holders to include providing a Privacy Act (e)(3) statement.</p> <p>DOC elected to not collect or use SSN's for the purchase card process, including using a uniquely created code as a default activation code or pin for purchase cards rather than the last four of a cardholder's SSN. DOC documented risk acceptance for the period between program transition and expiration of GSA ATO extension/issuance of new ATO for SP3 program. DOC has outlined a set of specific conditions for GSA and Citibank during this period to allow for processing of sensitive PII pertaining to DOC employees within the system.</p>
<input type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

<input checked="" type="checkbox"/>	<p>Yes, the conduct of this PIA results in required technology changes.</p> <p>Explanation: A process/solution for multi-factor authentication for DOC end users of the EAS was implemented. Enhancements were made to the existing Citibank encryption capability to protect information in transit between DOC and Citibank system(s).</p>
<input type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

## Points of Contact/Signatures

<p><b>Information System Security Officer or System Owner</b></p> <p>Name: Virna Winters Office: Office of Acquisition Management (OAM) Phone: 202.482.3483 Email: <a href="mailto:VWinters@doc.gov">VWinters@doc.gov</a></p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p> Signature: <u>VIRNA WINTERS</u> <small>Digitally signed by VIRNA WINTERS Date: 2020.08.31 18:08:29 -04'00'</small></p> <p>Date signed: _____</p>	<p><b>Information Technology Security Officer</b></p> <p>Name: Jerome Nash Office: Office of the Chief Information Officer (OCIO) Phone: 202.482.5929 Email: <a href="mailto:jnash@doc.gov">jnash@doc.gov</a></p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p> Signature: <u>JEROME NASH</u> <small>Digitally signed by JEROME NASH Date: 2020.09.01 13:26:37 -04'00'</small></p> <p>Date signed: <u>09/01/20</u></p>
<p><b>Privacy Act Officer</b></p> <p>Name: Lisa J. Martin Office: Office of Privacy and Open Government (OPOG) Phone: 202.482.2459 Email: <a href="mailto:Lmartin1@doc.gov">Lmartin1@doc.gov</a></p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <p> Signature: <u>LISA MARTIN</u> <small>Digitally signed by LISA MARTIN Date: 2020.09.01 18:07:37 -04'00'</small></p> <p>Date signed: _____</p>	<p><b>Authorizing Official</b></p> <p>Name: Lawrence Anderson Office: Office of the Chief Information Officer (OCIO) Phone: 202.482.2626 Email: <a href="mailto:landerson@doc.gov">landerson@doc.gov</a></p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p> Signature: <u>LAWRENCE ANDERSON</u> <small>Digitally signed by LAWRENCE ANDERSON Date: 2020.09.01 16:05:31 -04'00'</small></p> <p>Date signed: _____</p>
<p><b>Bureau Chief Privacy Officer</b></p> <p>Name: Maria Dumas Office: Office of Privacy and Open Government (OPOG) Phone: 202.482.5153 Email: <a href="mailto:mdumas@doc.gov">mdumas@doc.gov</a></p> <p>I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.</p> <p> Signature: <u>MARIA STANTON-DUMAS</u> <small>Digitally signed by MARIA STANTON-DUMAS Date: 2020.09.01 23:59:32 -04'00'</small></p> <p>Date signed: _____</p>	

**This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.**