

U.S. Department of Commerce



Privacy Threshold Analysis for the

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

U.S. Department of Commerce Privacy Threshold Analysis

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

Unique Project Identifier:

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44 U.S.C. § 3502(8).

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.

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) 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 DOC Bureau systems. NOAA ITC shares a secure interconnection with the Bureau of Census (CEN04-CBS) and NIST (CEN/CBS 162-01).

Additionally, a series of files will be transferred to support card monitoring and tracking. The Master ISA governs the entirety of all connections between Citibank systems and DOC systems, as well as any internal connections between DOC Bureau systems.

d) The purpose that the system is designed to serve

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. SmartPay 3 functions very similarly to SmartPay 2. 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 provide payment solutions to the agency employees to make purchases on behalf of their agency. DOC made an award to Citibank for purchase, travel, and fleet accounts.

To obtain a purchase account, an employee must be recommended by their supervisor, who then submits an application on their behalf through the program coordinator¹. 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.

e) The way the system operates to achieve the purpose

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. 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 the 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.

- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*

Information includes that which is necessary to provision a travel or purchase card, or in the management of those accounts and may include name, date of birth (DOB), contact information, including home and work address, phone number, and email, as well as financial information, including account number, credit card number, and financial transaction information. Additionally, employee ID and taxpayer ID are included in association with transactions. Finally, for Travel Card account holders, a Social Security number (SSN) is collected to verify identify of the individual associated with the account and to run a credit worthiness inquiry to determine what, if any restrictions will apply to the account.

- g) *Identify individuals who have access to information on the system*

Access will be available to cardholders, approving officials, and other officials with need-to-know in support of the DOC’s acquisition activities or in monitoring for appropriate use, fraud, waste, or abuse, or in compliance with applicable law(s) and regulation(s).

- h) *How information in the system is retrieved by the user*

Information is retrievable by a variety of fields within the information system to include employee name, card or account number, or transaction ID.

- i) *How information is transmitted to and from the system*

Information is transmitted between internal DOC systems and between DOC (NOAA) and Citibank systems via secure file transfer methodologies and as outlined in and governed by the Master ISA.

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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

_____ 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). *Continue to answer questions and complete certification.*

X 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). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

X Yes. *(Check all that apply.)*

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

_____ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

_____ Yes, the IT system collects, maintains, or disseminates BII.

X No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: “The term PII refers to 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.”

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

National Institute of Standards and Technology Associates

Contractors working on behalf of DOC

Other Federal Government personnel

Members of the public

No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, 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.

Provide the legal authority which permits the collection of SSNs, including truncated form. Consolidated Appropriations Act, 2008 (Pub. L. No. 110-161, Division D, Title VII, section 743), requires agencies to ensure a credit worthiness assessment is conducted of all new IBA travel charge card applicants prior to issuing a card. Under the GSA SmartPay Program, the contractor bank will conduct this assessment for the agency and advise the A/OPC as to whether a restricted or unrestricted card will be issued.

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the GSA Smartpay 3 system and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the GSA Smartpay 3 system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Virna Winters

Signature of ISSO or SO: VIRNA WINTERS Digitally signed by VIRNA WINTERS
Date: 2020.08.31 18:06:27 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jerome Nash

Signature of ITSO: JEROME NASH Digitally signed by JEROME NASH
Date: 2020.09.01 13:28:05 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Lisa J. Martin

Signature of PAO: LISA MARTIN Digitally signed by LISA MARTIN
Date: 2020.09.01 18:09:57 -04'00' Date: _____

Name of Authorizing Official (AO): Lawrence Anderson

Signature of AO: LAWRENCE ANDERSON Digitally signed by LAWRENCE
ANDERSON
Date: 2020.09.01 16:06:32 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Maria Dumas

Signature of BCPO: _____ Date: _____