Privacy Impact Assessment (PIA): CDC - CCPS - QTR3 - 2023 - CDC6823019

Created Date: 1/23/2024 3:01 PM Last Updated: 10/1/2024 4:02 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	CDC - CCPS - QTR3 - 2023 - CDC6823019	**PIA ID:**	1758732
Name of Component:	CDC - Credit Card Purchasing System	**Name of ATO Boundary:**	Credit Card Purchasing System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	211
Submission Status:	Re-Submitted	**Submit Date:**	2/2/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC6823019
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	2/23/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Secure Access Management System (SAMS) is the legacy auth provider and is no longer used. CCPS leverages Active Directory (AD) for auth provisioning.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	Credit Card Purchasing Systems (CCPS) is designed to provide information on account and credit card purchases. CCPS provides end to end purchase order life cycle management and automates the logging, tracking, and obligation of credit card transactions and purchase requests and support dynamic work flow management and request tracking.

PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	CCPS does contain sensitive information in the form of CDC Credit Card transactions , credit card holder's information including name, date of birth, phone number, mailing address, email address, and last 4 digits of Social Security number (SSN). Other information CCPS collects not classified as sensitive is vendor and fund authorization information to include: National interest category (e.g., Haiti Earthquake), whether the purchase is for supplies, date the supplies are due to CDC, whether the purchase is for services, date the service will be completed, Product Service Code, General Services Administration (GSA) (or other agency contract number), Vendor's information (including Vendor identification number), address, point of contact information, Domestic or Foreign Entity, FedBizOpps solicitation number (if applicable), if the purchase competed, and how many offers received. CCPS receives purchase transaction records, demographic, and invoice files from the financial Institution's bank via Data Management and Analytics Support (DMAS). DMAS is a separate system with its own approved PIA. CCPS does archive and process the last 4 digits of card holder SSN, however unmasked SSNs from the financial institution will not come to the CDC's boundary. User's log in using the Active Directory which is a separate system covered by its own PIA. User IDs are stored within Active Directory.
PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	
PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	Credit Card Purchasing Systems (CCPS) automates the logging, tracking and obligation of credit card transactions and purchase requests. It collects request for purchase and items to be purchases, its all approval personal approval name, date of approval and Card holder purchase information from merchant/vendor, Citi Bank transaction record as daily input and documents related to purchase invoice and other approval documents. All the information gathered by CCPS is needed to assist the system in performing its primary duties of logging, tracking, and obligation of credit card transactions and purchase requests, as well as matching request log data to bank transactions. User's log in using the Active Directory which is a separate system covered by its own PIA. User IDs are stored within Active Directory.

PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	Credit Card Purchasing System (CCPS) (http://CCPS.cdc.gov) provides end to end purchase order life cycle management and automates the logging, tracking, and obligation of credit card transactions and purchase requests and support dynamic workflow management and request tracking. CDC employees access the link through Active Directory.
PTA - 10:	Does the website have a posted privacy notice?	No
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No

PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Truncated SSN Name Email Address Phone numbers Date of Birth Mailing Address Financial Account Info
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	PII is used to uniquely identify card holders. The last four digits of the SSN is used to match with the financial institution's data. The full SSN is not imported into the CCPS database nor is it available in the CCPS application. The bank uses this as a unique identifier, and no unmasked SSNs will ever enter CCPS's boundary.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	The last four digits of the SSN is used to match with the correct credit card holder with the bank data.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Executive Order 9397 (only last four digits)
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Budget and Accounting Act of 1950 (Pub. L. 81-784); Debt Collection Act of 1982 (Pub. L. 97-365); Debt Collection Improvement Act of 1996 (Pub. L. 104-134, sec. 31001); E.O. 9397; E.O. 12931, and 40 USC, Sections 501-502
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Employee name / User ID
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	GSA/GOTV 6 GSA Smartpay Purchase Charge Card Program 09-90-0024, Financial Transactions of HHS Accounting and Finance Offices

PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A This system does not process from or about the general public.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	PII is shared with approvers and auditors for validating credit card transactions and vendor information is shared with HHS to document payments.
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	There is an Interconnection Security Agreement (ISA) between CDC and the financial System Unified Financial Management System (UFMS) owned by Health and Human Services (HHS) to address the use of data within the system.
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	The procedure that the Interconnection Security Agreement (ISA) outlines is for the credit card purchases that are pushed from CDC to HHS UFMS. There are audit logs available for identification in the event of a third party request within CCPS.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	The use of PII is required for an employee who wants to participate in the GSA SmartPay VISA purchase Card Program. If the employee does not want to share PII, he or she cannot obtain a government sponsored credit card.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	Any changes to the system would be driven by the needs of GSA SmartPay VISA Purchase Card Program administered at CDC by the OFR. The Program administrator at CDC/OFR notifies all program participants and CCPS users of program changes, and their related impact to CCPS via email.

PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Users are to contact the administrator at CDC/OFR for the GSA SmartPay VISA Purchase Card Program. They can also send an email to the CDC Purchase Card mailbox at cdcpurchasecard@cdc.gov.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	CCPS is updated daily with PII Changes reported to the credit card company. This ensures the data's consistency with the system of record at the credit card company.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: To Log and Track their CDC Visa Card Transactions only. Administrators: To assist users in logging and tracking their CDC VISA card transactions, and to import and export transactions. Contractors: Direct contractors who are developers have access to PII in order to fix bugs and perform updates or changes to the system.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	A user's access to PII is enforced via role based access control. Permissions are assigned to CCPS roles, and users are assigned to roles with the lowest level of permissions necessary to complete their job. The CCPS Product Owner is the authorized approver for CCPS roles. All role requests must originate or be approved by the CCPS Product Owner or designated representative. Upon verification of approval, the role requests will then be routed to the System Administrators, who will assign users to those roles.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	Access to information is based on user role within CCPS. Each user role is limited to only the information needed to perform that role-based function. The least privileged model is utilized and is authorized by the CCPS Product Owner or designated representative.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	All CDC personnel are required to take Security Awareness Training(SAT) and Privacy Training at least annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	None

PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	All official records are transferred or destroyed based on CDC record management policies and practices. The following records schedules apply to the system: GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative Controls: The system utilized Azure file backups, Least privilege access, and user manuals. All CDC Personnel are required to take Security Awareness Training(SAT) and Privacy Training at least annually. Technical Controls: Access to the system and to specific information is controlled using windows integrated Authentication via Azure Gov Cloud AD services, so users have to have a valid and active network profile before they are allowed system access. Network and security controls for the web services and databases are in place as well as network security monitoring and security audits. The system is only available on the Intranet, mitigating the exposure outside the firewall. Physical Controls: Controls are managed by security guards, ID Badges, locked doors and key card restrictions.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	2/5/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: February 5, 2024	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	2/6/2024
		SOP Days Open:	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/8/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Signature.docx
SAOP Comments:	Approved on behalf of Bridget Guenther	**SAOP Review Date:**	3/1/2024
		SAOP Days Open:	22

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	1/23/2024	Please also select "truncated SSN" and "email address"	
PIA - 10C	Data Feed Service, piafrmcdc	1/23/2024	Please include a justification (can be as simple as "this system does not process from or about the general public"	
PIA - 23	Data Feed Service, piafrmcdc	1/30/2024	Please update the retention schedule. These citations no longer exist.	
PIA - 1	Data Feed Service, piafrmcdc	10/1/2024	This System has been migrated within the OCIO Azure GSS authorization boundary. All future updates should be made via the new Sub- Component application.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	10/1/2024 4:02 PM	**History Log:**	View History Log