Privacy Impact Assessment (PIA): OS - MACCS - QTR1 - 2025 - OS2372751

Created Date: 4/4/2025 5:03 PM Last Updated: 4/15/2025 1:23 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:	OS - MACCS - QTR1 - 2025 - OS2372751	**PIA ID:**	2968845
Name of Component:	OS - OS - OS - Managing & Accounting Credit Card System	**Name of ATO Boundary:**	Managing & Accounting Credit Card System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	48
Submission Status:	Submitted	**Submit Date:**	4/3/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	OS
Security Categorization:		**OpDiv PIA ID:**	OS2372751
Legacy PIA ID:		**Make PIA available to Public?:**	No

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.	
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.
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?
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.
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.
PTA - 5A:	Are user credentials used to access the system?
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.
PTA - 7:	Does the system collect, maintain, use or share PII?
PTA - 7A:	Does this include Sensitive PII as defined by HHS?
PTA - 8:	Does the system include a website or online application?
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?

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.
PTA - 10:	Does the website have a posted privacy notice?
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?
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?
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?
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?
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?
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Financial Account Info Other - Free text Field - HHS ID and Agency.
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.	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	The primary use of PII information is to enable role-based and rule-based access and allow users to reconcile their credit card purchases.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There is no secondary use of PII.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC 301, Departmental regulations.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
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.	
PIA - 9:	Identify the sources of PII in the system.	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
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
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)).	
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.	
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.	Credit cards are issued by Citi bank and the PII data is transmitted to the Managing and Accounting Credit Card System (MACCS) system. Opting out would result in them not being able to obtain the credit card and will not have access to MACCS.
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.	For general changes to the MACCS System, we would notify users on the upcoming changes through mass email communication detailing the upgrades.
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.	MACCS only collects PII for the purposes of system access and authorization. If the process owner or stakeholder believes that the PII is inappropriately obtained, used, or disclosed or that the PII is inaccurate, MACCS team members will investigate and redirect the process owner/stakeholder to the Citi bank team to resolve the concern. Customer support email account fms_dfo_tieriihelpdesk@psc.hhs.gov can be used to open a ticket.
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.	The process for periodic review(s) of PII is out of scope and not our responsibility to maintain. The MACCS system relies on the accuracy of the data provided by Citi bank.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	The system administrator(s) will need to see the users' first and last name including email address in order to resolve any issues with the user's credit card transaction or their posting in financial management system
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The administrative procedures are as followed: System Administrators are selected to perform standard system procedures such as verifying user's PII data and if not, informing Citi bank to correct it on their end. Accuracy with the PII data is essential for authentication and authorization for performing user's reconciliation.
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.	The technical method in place includes minimal share of user information (coming from the Citi bank) to allow the system administrators to perform their job(s).
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 system administrators are required to complete the "Introductory Role-Based Training for IT Administrators" along with submitting their certificate of completion before they are granted access to the MACCS system. All system administrators are required to complete this training annually.

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All system administrators are required to complete the "Introductory Role-Based Training for IT Administrators", along with receiving an approved Tierr 4 investigation, and may include an elevated account request to the system for additional configuration. All system administrators are required to comply with additional security and privacy awareness training as well.
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).	General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. MACCS will also maintain audit logs and will dispose of them after 2 years.
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: The system will secure PII through role-based and rule-based access controls and permissions which are set at the account level. Managing and Accounting Credit Card System (MACCS) will only have limited information (First Name, Last Name, Email Address) in the system to enable system administrators to perform their designated role. MACCS also uses Access Management System (AMS) Multifactor authentication with access limited to PIV card only. Technical: PII is encrypted in transit and at rest. PII captured within an MACCS is also obfuscated. Physical: The system is a software as a service system, but physical controls are in place within the Sev1Tech/AWS data centers.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/4/2025
Privacy Analyst Comments:	Vanessa, this PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	4/4/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	4/15/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 4/15/2025 We requested the exported PIA from OS because the PTA in Archer didn't sync it was blank. The PIA was review externally and approved outside the tool. The Approved PIA is attached to the OS Archer record in supporting Documentation.	**Agency Privacy Analyst Days Open:**	11

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer_Signature_Crystal_Bland.docx
SAOP Comments:	PIA Approved outside the tool. PTA didn't sync to OIS instance.	**SAOP Review Date:**	4/15/2025
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
4-15-2025 MACCS_OS2372751_Approved.pdf	276147	.pdf	4/15/2025 1:21 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmos_Release	4/2/2025	Please leave a comment for the question in the general information	

			section that did not populate a response: 4: ATO Date or Planned ATO Date.
PIA - 1	Data Feed Service, piafrmos_Release	4/2/2025	Based on the information provided in the PTA and PIA this response should be updated with additional selections. Select 'Other - Free text field' and please include 'HHS ID' and 'agency as these are listed in the PTA. Please also select 'Financial Account Info' as the PTA/PIA indicates this is collected and used: MACCS collects cardholder user data, credit card and transaction data from Citi bank. It also collects Common accounting number (CAN) and Object Class (OC) data from Unified Financial Management System (UFMS) Transaction data: Purchase date, process date, transaction reference number, merchant, amount.
PIA - 7	Data Feed Service, piafrmos_Release	4/2/2025	The following information was included in the response to the previous PIA on record. If any of this information is still pertinent, please include it in the updated response: Financial and related activities are authorized by the Budget and Accounting Act of 1950 (Pub. L. 81-784); Debt Collection Act of 1982 (Pub. L. 97-365); and the Debt Collection Improvement Act of 1996 (Pub. L. 104-134, sec. 31001).
PIA - 11	Data Feed Service, piafrmos_Release	4/2/2025	It is indicated in the PTA/PIA that information is collected/provided from Citi bank and cards are issued by them. Is any information provided back to Citi back by the system? If yes, please update this response as well as the subsequent responses regarding information sharing.
PIA - 13	Data Feed Service, piafrmos_Release	4/2/2025	Please define the acronym 'MACCS' on first use within this response. And please add a period to the end of the last sentence.
PIA - 24	Data Feed Service, piafrmos_Release	4/2/2025	Please define the acronyms 'AMS', and 'AWS' on first use within this response.

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:	4/15/2025 1:23 PM	**History Log:**	View History Log