Privacy Impact Assessment (PIA): CDC - OAP - QTR1 - 2024 - CDC7412826

Created Date: 3/21/2024 12:01 PM Last Updated: 11/7/2024 7:01 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 - OAP - QTR1 - 2024 - CDC7412826	**PIA ID:**	1787319
Name of Component:	CDC - OFR Appian Platform	**Name of ATO Boundary:**	OFR Appian Platform
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	293
Submission Status:	Re-Submitted	**Submit Date:**	10/22/2024
Next Assessment Date:	11/07/2027	**Expiration Date:**	11/7/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC7412826
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.	9/15/2025
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.	There have been no significant changes to the system since the last PIA.
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.	The OFR Appian Platform (OAP) consists of 2 systems covered by this PIA, the Acquisition Performance and EXecution (APEX) System and the Resource Management System (RMS). The Acquisition Performance and EXecution (APEX) system will provide the Centers for Disease Control and Prevention (CDC), through the Office of Financial Resources (OFR), a single system for managing the full procurement cycle from procurement request to closing out a contract for all types of procurements. Its function is to meet the following Integrated Acquisition objectives: 1. Integrated acquisition automation tool and streamlined processes 2. Reducing cycle times for all types of procurement actions 3. Accurate, real-time acquisition related information that can be used by management to make strategic and planning decisions 4. Ability to integrate with standard government wide standard requirements The Resource Management System (RMS) automates the requesting and planning of budgets, funding sources, and object class level details. RMS is a budget-centric system, in a web-based (.NET) environment. Its function is to meet the following objectives: 1. Purchase Order Requisitioning And Award 2. Contracts Requisitioning And Award 3. Receiving Property 4. Receiving Requiring Payment Authorization 5. De-obligations / Modifications 6. Contract Closeout RMS automates the Budget Planning, Forecasting, and Formulation processes at the budget, funding sources, and object class level details. RMS is a suite of applications covering a wide range of functions to assist CDC management in Planning, Forecasting, Formulation, Acquisition and Assistance Planning, and Reporting.

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.	The Acquisition Performance and EXecution (APEX) system will collect the following types of data for the purpose of managing the full procurement purposes: 1. Purchase Order Award and Contract Requisitioning Award 2. Receiving Property 3. Receiving Requiring Payment Authorization 4. De-obligations / Modifications 5. Contract Closeout 6. Business owner names 7. Email addresses 8. Employer ID numbers (EIN) which may sometimes be the Social Security Number (SSN). Though the system does not require the SSN, it is possible that some small businesses may use their SSN as their EIN. The Resource Management System (RMS) is a one-stop shopping tool for daily financial reporting, budget and staffing planning, and procurement forecasting. The RMS databases contain the following Personable Identifiable Information (PII): 1. Name 2. Employee Status 3. Payroll Status for purposes of identifying employees The RMS application and associated databases do not collect, process, store or maintain SSNs. Authentication for APEX and RMS will be achieved through rights assigned in the MS Windows Active Directory (AD). MS Windows AD is a CDC system that has its own PIA.
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.	HHS User Credentials HHS/OpDiv PIV Card
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.	Acquisition Performance and Execution (APEX) collects name, email address, and EIN for procurement purposes including purchase order requisitioning, contracts requisitioning, receiving property, receiving payment authorization, De-obligations and Modifications, and Contract Closeout. The Resource Management System (RMS) databases collects Name, Employment Status, and Payroll Status for purposes of identifying employees. Authentication will be achieved through rights assigned in the Microsoft (MS) Windows Active Directory (AD).
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?	
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.	The Acquisition Performance and EXecution (APEX) and Resource Management System (RMS) application are web-based architecture that resides on Appian's Platform as a Service (PaaS). The platform is managed by Appian and supported by a support team that is responsible for the operational stability, patching, and upgrades of the platform. The platform resides in the Amazon Web Services (AWS) GovCloud East region in a single availability zone. The APEX and RMS application is built on Appian's low-code platform consisting of an Integrated Development Environment (IDE) that provides the configuration of user interfaces, business processes, rules, federated records, and integrations to external databases and web services.
PTA - 10:	Does the website have a posted privacy notice?	Yes
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.	Social Security Number Name Email Address Employment Status Other - Free text Field - Employer Identification Number (EIN) and Payroll Status
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Vendors/Suppliers/Third-Party Contractors (Contractors other than 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?	Personally Identifiable Information (PII) is used for tracking.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Personally Identifiable Information (PII) is also used for communication with the vendor, including payment. The Resource Management System databases contain the following PII items: Name, Social Security Number (SSN), Employment Status, and Payroll Status for purposes of identifying employees and processing Labor Distribution System (LDS) transactions.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	To the extent that the Social Security Number (SSN) is captured, it is reported by the vendor as their Employer Identification Number (EIN) and serves that function. The Acquisition Performance and EXecution (APEX) systems purpose is not specifically to collect Personally Identifiable Information (PII) however, some small businesses may use personal information as their employee numbers. This can possibly introduce their SSN as their EIN. SSNs are passively stored, collected and or maintained due to the usage of them by a business owner as the EIN. Resource Management System SSNs are viewed for entry into the Accounting for Pay System (AFPS) to process over 13,000 Labor Distribution System (LDS) transactions.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Executive Order 9397.

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Title 31 United States Code (U.S.C. 3512, 3711, 3716, 3721, 1321 note; Executive Order (E.O.) 13520.
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.	Directly from an individual about whom the information pertains Online 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 - information is not sourced or collected from the public.
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.	None. The Acquisition Performance and Execution (APEX) system was created for the purpose of being a single system for managing the full procurement cycle, and since information in the system is collected from the documentation submitted by contract awardees, individuals do not have the option to consent to particular uses of their information once it is collected into the system. Though applying for the contract is voluntary, if individuals were to opt out of providing this basic information, then they could be determined ineligible to receive the contract award, if they refuse to share their data.

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.	Individuals providing information that is ultimately collected by this system would be provided notice at the time of the contract award using Privacy Act Statements that inform them of the authority for and purpose of the collection, the uses for which the information will be shared, and whether providing the information is mandatory or voluntary. Notice is also provided by this Privacy Impact Assessment (PIA), and any significant change would be described within a new, revised PIA.
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.	Individuals with concerns about the use of or disclosure of their CDC userid, first name or last name, may contact the Director of Financial Resources (OFR) at 678-475-4500, who will respond appropriately within 30 days. If the user believes their information was improperly disclosed, OFR will investigate whether or not the disclosure occurred and if so, apply appropriate measures to ensure it does not happen again. If the user does not wish to have their information included in the system, OFR will remove their information along with their access to Acquisition Performance and EXecution (APEX) and/or Resource Management System (RMS). The only way to eliminate the use of this information would be removal from the application at the request of the individual or their leadership.
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 system is an automated acquisitions tool that essentially documents the process. As such, business rules are employed throughout the system to verify the accuracy of the transactions.
PIA - 17:	Identify who will have access to the PII in the system.	Developers 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.	Developers - Have access to the system for the purposes of maintenance, bug-fixes, and changes. Contractors - The developers are direct contractors who may have access to PII for development.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Each user account is assigned certain roles with a defined set of privileges to ensure overall system integrity. Access is limited to OFR personnel who have a need to access the system based on their roles in support of system development and maintenance for the purpose of changes or bug fixes.

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 roles and privileges assigned to a particular user are predetermined depending on the user's function. Role Based Access Controls with least privilege methods limit the amount of information the user can see to-perform their duties.
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/OFR personnel complete mandatory privacy and security 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).	Destroy when 5 years old or when no longer needed for administrative purposes, whichever comes first. GRS 1.1 Item# 010. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis.
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: Records are maintained according with CDC's record control schedule and record control policy. The PII is secured using the CDC/IS Active Directory authentication process and role-based application control via Role Based Access Control (RBAC). Technical: Monitored by the Network and IT security controls which is administered by Cybersecurity Program Office (CSPO) and Digital Services Office (DSO). Physical: 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:**	10/23/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	10/24/2024
		SOP Days Open:	2

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/31/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 10/31/2024 All comments have been addressed. This PIA is ready for SAOP review and approval. 9/24/2024 Per Email (see Supporting Documentation), PTA-8 response should be "Yes." All other comments have been addressed. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	7

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	11/7/2024: Comments were resolved. 10/2/2024: EIN and payroll status are listed as PII elements in PTA-5, so they should be included in PIA-1. CDC updated PIA-1 and for the Dept PIA Analyst review, in PIA-1 Other was selected and EIN and payroll status were in the free text. However, in the SAOP view EIN and payroll status are no longer in the free text. Looks like the history log and for whatever reason the data feed wipe out that selection. We are rejecting the PIA to have CDC fix PIA 1 to include EIN and payroll status on their end and resubmit back to us and see if the data feeds let it stick.	**SAOP Review Date:**	11/7/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Re_ CDC - OAP - QTR1 - 2023 - CDC6711531.pdf	232681	.pdf	9/24/2024 1:27 PM	1

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 6	Data Feed Service, piafrmcdc	3/25/2024	EIN isn't PII while SSN is PII. Are SSNs of individual people collected or EINs of organizations?	
PIA - 6	Data Feed Service, piafrmcdc	8/26/2024	Please clarify whether EIN stands for employee identification number or employer identification number.	
PIA - 1	VILLAFUERTE, NESTOR	9/19/2024	Reviewer notes that PTA-8 failed to sync. Please include EIN in your response.	
PIA - 1	BLAND, CRYSTAL	9/20/2024	Please include payroll status in your response.	
PIA - 1	Data Feed Service, piafrmcdc	10/22/2024	Employer Identification Number (EIN) and Payroll Status was added.	
PIA - 6	Data Feed Service, piafrmcdc	10/22/2024	EIN stands for Employer Identification Number. Social Security Numbers (SSNs) are passively stored, collected and or maintained due to the usage of them by a business owner as the EIN. Resource Management System SSNs are viewed for entry into the Accounting for Pay System (AFPS) to process over 13,000 Labor Distribution System (LDS) transactions.	

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:	11/7/2024 7:01 PM	**History Log:**	View History Log