Privacy Impact Assessment (PIA): CDC - AWS-GC-01 - QTR2 - 2024 - CDC8270758

Created Date: 5/15/2024 8:03 PM Last Updated: 6/14/2024 4:25 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 - AWS-GC-01 - QTR2 - 2024 - CDC8270758	**PIA ID:**	1828551
Name of Component:	CDC - AWS GovCloud OCIO DSO GSS	**Name of ATO Boundary:**	AWS GovCloud OCIO DSO GSS
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	31
Submission Status:	Submitted	**Submit Date:**	5/15/2024
Next Assessment Date:	N/A	**Expiration Date:**	6/14/2027
Office:		**OPDIV:**	CDC
Security Categorization:		**OpDiv PIA ID:**	CDC8270758
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	11/30/2024
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.	New
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?	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.	AWS GovCloud is a cloud-based General Support System (GSS) composed of virtual servers, firewalls, operating system software, data, and network infrastructure components. The platform supports system development, testing, and production instances of various CDC applications, security services, websites, analytical tools, backup and storage platforms, and high-performance computing. The platform is built on the Federal Risk and Authorization Management Program (FedRAMP) approved Amazon Web Services (AWS GovCloud) Infrastructure that provides a shared pool of configurable AWS computing resources such as servers, storage, network infrastructure, applications, and various services.

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.	This system is an infrastructure platform. As such, its purpose is not to collect and maintain data; instead, all data will be stored at the child application level and a separate Privacy Impact Assessment (PIA) will be submitted for consideration for each application capturing the specific type of information stored and maintained. AWS GovCloud collects and stores contractor system administrator user identifier, passwords and email addresses (they are considered "Direct Contractors") and also stores system-related information about the systems that are deployed; i.e., log files API (Application Program Interface) logs including potential usernames. AWS GovCloud User identification is administered through CDC Active Directory (AD), a separate system with its own PIA.
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.	AWS GovCloud is a managed cloud platform operated by the CDC Office of the Chief Information Officer (OCIO) on behalf of the CDC. The platform supports development, testing, and production instances of various CDC applications, security services, websites, analytical tools, backup and storage platforms, and high-performance computing. As an infrastructure platform, the system provides the hosting and maintenance for CDC applications, each of which will have its own separate PIA. This system is an infrastructure platform. As such, its purpose is not to collect and maintain data; instead, all data will be stored at the child application level and a separate Privacy Impact Assessment (PIA) will be submitted for consideration for each application capturing the specific type of information stored and maintained. AWS GovCloud collects and stores contractor system administrator user identifier, passwords and email addresses (they are considered "Direct Contractors") and also stores system-related information about the systems that are deployed; i.e., log files API (Application Program Interface) logs including potential usernames. AWS GovCloud User identification is administered through CDC Active Directory (AD), a separate system with its own PIA.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	No

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?	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.	Email Address User Credentials

PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors 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.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	The primary use for the PII in AWS GovCloud will be to identify, authenticate and authorize individuals accessing and associated with each workflow in the system.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Modernizing Government Technology Act of 2017
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 Email Online
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.	This system does not collect information 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.	There is no option to opt out. System administrators understand that opting out is associated with their access credentials being terminated.
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.	AWS GovCloud does not collect PII directly from individuals. Users of the system are required to maintain active information in the Active Directory (AD) which has its own 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.	In the event that PII has been inappropriately obtained, used, or disclosed, the affected person(s) would escalate this concern to the contractor project manager in writing. The contractor project manager would engage with the appropriate channels to investigate the root cause and work on a process for resolution. Individuals may contact Cybersecurity Program Office (CSPO) Help Desk at 508helpdesk@cdc.gov if they believe their PII has been inappropriately obtained, used, disclosed or is inaccurate.
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 integrity, availability, accuracy and relevancy of the data is ensured because the administrators (whose PII is contained in the system) are charged with reviewing, monitoring and ensuring that new accounts are setup and terminated as necessary. As a result, outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system.
PIA - 17:	Identify who will have access to the PII in the system.	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.	Administrators: Provide system administration and maintenance. Direct Contractors require access in order to provide system administration and maintenance.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Designated System Administrator access is determined by the staffing of the project. Access is role-based and is managed by the contractor project manager.
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.	Individuals with appropriate role-based access are allowed to review but are limited by their role-based access in terms of what PII can be viewed. The established policy is that System Administrators have access to each other's email address that are used as stored usernames in the system. However, they do not have access to each other's passwords.

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 employees and contractors are required to complete annual Privacy and Security Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Administrators hold industry certification for various components in their field of expertise.
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).	The General Records Retention GRS 5.1 item 020 (DAA-GRS-2016-0016-0002) applies: Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.
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 Administrative controls include the enforcement of user roles and by having users agree to system Rules of Behavior. Any changes to the system must go through the CDC Change Management Process. All administrators must take the annual required privacy training. Technical Controls Technical controls are in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system. The system utilizes role-based access and grants access to the data based on authentication and authorization. AWS GovCloud user identification is administered through CDC Active Directory (AD). Intrusion detection sensors to monitor network traffic and report events; security logging; and alerting system. Firewalls, secure access points, intrusion detection, and transmission protection. Multi-factor authentication for system and data center access. Physical controls: Servers are housed in a third-party vendor data center. Physical access is strictly controlled by both perimeter and building ingress points. The facility has physical security staff, video surveillance, intrusion detection system, and two-factor authentication for access to data center floors.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/15/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor)	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	6/10/2024
		SOP Days Open:	26

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	6/11/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/11/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	6/14/2024
		SAOP Days Open:	3

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	6/11/2024	On the next iteration of the PTA please provide response for PTA-5A and PTA-5B, if applicable.	

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:	6/14/2024 4:25 PM	**History Log:**	View History Log