Privacy Impact Assessment (PIA): CDC - CITI - QTR1 - 2024 - CDC7810146

Created Date: 2/21/2024 7:02 PM Last Updated: 3/1/2024 3:01 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 - CITI - QTR1 - 2024 - CDC7810146	**PIA ID:**	1769993
Name of Component:	CDC - CSPO IT Infrastructure	**Name of ATO Boundary:**	CSPO IT Infrastructure
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	21
Submission Status:	Re-Submitted	**Submit Date:**	2/26/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC7810146
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.	4/22/2024
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.	No changes to the PIA since last submission.
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 CSPO IT Infrastructure (CITI) consists of the systems used for monitoring applications, network traffic, backup and recovery, creates a frozen snapshot of a workstation's desired configuration and settings and machine configurations for compliance with the security policies. This gives personnel the ability to facilitate a process during events and incidents. CITI also allows remote scanning for patch compliance and deployment of any patches deemed necessary on various computer systems.

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 type of information the system will collect, maintain (store), or share is network traffic and information from each server or workstation. CITI also contains Cybersecurity Program Office (CSPO) created policies and support information as well as the results of malware analysis. The system also collects names and versions of software installed on computers. The system will be backing up data stored on CSPO user share drives, and servers supporting Policy, Incident Response and Forensic data. Data elements stored within the network storage, or physical tape library, can include user information, PII, and any other forensic information needed as investigations permit, although no passwords are stored on any of the data that is backed up or stored. PII could possibly include Social Security Numbers, Name, Drivers License Number, Mother's Maiden Name, Email Addresses, Phone Numbers, Medical Notes, Certificates, Education Records, Military Status, Foreign Activities, Taxpayer ID, Date of Birth, Photographic Identifiers, Biometric Identifiers, Vehicle's Identifiers, Mailing Address, Medical Records Number, Financial Account Legal Documents, Device Identifiers, Employment Status, and Passport Number. Authenticates with CDC's Active Directory domain controllers. Active Directory is a separate system covered by a separate Privacy Impact Assessment (PIA). No local accounts/credentials are generated to allow access this system. User credentials are managed in accordance with CDC policy. Only privileged user accounts are allowed to access to the system and those privileges are controlled by CSPO Support administrators.
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.	PII could possibly include Social Security Numbers, Name, Drivers License Number, Mother's Maiden Name, Email Addresses, Phone Numbers, Medical Notes, Certificates, Education Records, Military Status, Foreign Activities, Taxpayer ID, Date of Birth, Photographic Identifiers, Biometric Identifiers, Vehicle's Identifiers, Mailing Address, Medical Records Number, Financial Account Legal Documents, Device Identifiers, Employment Status, and Passport Number. Digital Services Office (DSO) is used for data backups of the CSPO Forensic and Support as well as other critical CSPO systems and data. Data elements stored within the network storage, or physical tape library, can include user information, PII, and any other forensic information needed as investigations permit. Data can be stored on network storage, or physical tape storage, for a period ranging from one week to one year. Forensic data is generally stored for upwards of several years. No direct contractors gain access to this system. Authenticates with CDC's Active Directory domain controllers. Active Directory is a separate system covered by a separate Privacy Impact Assessment (PIA).
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.	Website is only available on the intranet and is not browsable. Access to webpage has to be granted for CITI/Bigfix application admins only. Any attempt to browse to the URL is immediately blocked. Primarily provides a web api for Splunk ingestion.
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.	Social Security Number Truncated SSN Name Mother Maiden Name Email Address Phone numbers Medical records (PHI) Certificates Education Records Military Status Foreign Activities Date of Birth Photographic Identifiers Biometric Identifiers Vehicle Identifiers Mailing Address Medical Records Number Financial Account Info Legal Documents Devices Identifiers Employment Status Passport Number User Credentials Patient ID Number Driver License Number
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.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	Digital Services Office (DSO) backs up file servers for Centers/Institute/Offices at CDC that contains Personally Identifiable Information PII related to each C/I/O mission.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Uses of PII are varied but consistent with CDC functions and activities. Uses could include system authentication purposes, internal and administrative human resource functions or any of a multitude of other activities that CSPO conducts.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable-SSN is not specifically collected, it can be included in Cybersecurity Program Office (CSPO) data
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable as collection is only due to CSPO IT Infrastructure as an information storage system, SSN is not used as such. Each system that has data stored inside CITI has a seperate PTA/PIA.

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Public Law 99-474
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.	Government Sources Within the OPDIV Other HHS OPDIV
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.	Not Applicable as collection is only due to CSPO IT Infrastructure as an information storage system, OMB information collection approval would not apply as each system that has data stored inside CITI would have seperate PTA/PIA documentation.
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.	This system does not solicit personal information from individuals, and so, does not provide notice to individuals about what information is collected or how it is used. The CDC Network Logon banner provides a system use notification which includes the statement, " You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose." Additionally, all CDC users are required to complete on an annual basis a Rules of Behavior (ROB) which also explains proper operation and expectations while using the Network.
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.	No PII is specifically collected or used through the use of the system; therefore, there are no notifications to users about PII data and no consent obtained to use it. The notification and consent process is part of the underlying business practices governing use of the system.
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 may contact the CDC Computer Security Incident Response Team (CSIRT) via email or by phone. 1.866.655.2245, CSIRT@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.	No processes are in place for periodic reviews. The data collected will not be systematically checked for such, but information collected is considered an accurate representation of the content as of the time of collection. Data is pulled directly from network.
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.	Administrators do not require access to PII to fulfill job functions, however their role enables access to view data during backup process.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role Based Access Control (RBAC) procedures are in place and assigned via management to ensure that only authorized users and administrators are able to access information.
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.	Least Privilege is used and assigned via management to ensure that administrators access only the information needed to complete job functions.

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 users are required to complete CDC Security and Privacy Awareness Training annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Role Based Training is required for any privileged users.
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).	At no time should any artifact related to the incident be deleted – should space run out on the Forensic file share, all case files should be archived to offline storage. This policy supports both the ability to perform historical research into security incidents at a later date and compliance with the U.S. National Archive and Records Administration (NARA) General Records Schedules (GRS). Per NARA directives, forensic evidence must be maintained for a minimum of three years . DAA-GRS2013-00060002
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: Mandatory Security and Privacy Awareness Training for all users. Role Based Training required for any Privileged Users Technical: Implement Role Based Access Controls based on AD permissions. The system employs encryption and non-repudiation through the support of digital signatures and encrypted email using PIV. Physical The physical controls, implemented by the system, restrict access to CDC buildings and areas housing computers used by this system. These controls include security guards, identification badges, key cards, locked doors, cipher locks, fences, alarms and closed-circuit TV. Also there are Emergency shutoff systems, and fire and water damage protections.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	2/26/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: February 26, 2024	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	2/28/2024
		SOP Days Open:	2

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/29/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski Attached exported PIA in Supporting Documentation to confirm responses that did not sync over for PTA-5A response is "Yes, but maintain in another system" PTA-8 response is "Yes." This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

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:	1

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Copy_of_CITI Privacy_Impact_Assessment_PIA_bl (4).rtf	210822	.rtf	2/29/2024 4:14 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 24	Data Feed Service, piafrmcdc	2/21/2024	Please modify answer.	
PIA - 23	Data Feed Service, piafrmcdc	2/21/2024	This citation is for "Computer Security Incident Handling, Reporting and Follow-up Records". Is this correct? It does not align with the rest of this submission. Please review and confirm citation.	
PIA - 1	LASKOWSKI, JAMES	2/29/2024	The reviewer notes that PTA 8 did not sync.	
PIA - 4	LASKOWSKI, JAMES	2/29/2024	Please spell out C/I/O on first use.	
PIA - 4	KORAN, ELIZABETH	3/1/2024	Reviewers understand that C/I/O refers to Centers/Institute/Offices. In next iteration, please define the acronym immediately after the words to ensure clarity for the public.	

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:	3/1/2024 3:01 PM	**History Log:**	View History Log