Privacy Impact Assessment (PIA): CDC - CVTM - QTR1 - 2024 - CDC8044093

Created Date: 3/15/2024 4:01 PM Last Updated: 4/17/2024 8:02 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 - CVTM - QTR1 - 2024 - CDC8044093	**PIA ID:**	1782340
Name of Component:	CDC - CSPO Vulnerability and Threat Management	**Name of ATO Boundary:**	CSPO Vulnerability and Threat Management
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	35
Submission Status:	Re-Submitted	**Submit Date:**	3/21/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	High	**OpDiv PIA ID:**	CDC8044093
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.	12/8/2026
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.	System have been upgraded from a Moderate to High system Categorization and the presence of PII being stored in one of the tools. Sensitive PII is not stored in the system. (Updated BSI have been uploaded)
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.	CSPO Vulnerability and Threat Management (CVTM) is a valuable enterprise tool used in support of the Department of Homeland security (DHS) Continuous Diagnostics and Mitigation (CDM) Program to meet the following requirements: hardware asset management (HWAM), vulnerability management, and compliance management. CVTM is comprised of multiple network monitoring tools that together detect and block traditional and next generate web-based threats and attacks. CVTM a continuous monitoring program scans for deficiencies of the CDC network; such as compliance, vulnerability, and patch management, Network Security Monitoring, Logs, Application Scanning System, and Snort sensor data management
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.	CVTM collects data necessary to determine network diagnostics and vulnerability mitigation as a result of continuously scanning and monitoring the CDC network, such as date; time; system name; IP address (Not link to individuals); Operating System; vulnerability identification numbers and descriptions; and software version numbers. System also collect and store User names and Identification.
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.	CVTM is used to assess the security posture of the CDC Enterprise network by providing the capability to continuously scan and monitor the network for security vulnerabilities and weaknesses. CVTM collects and stores: date; time; system name; IP address; Operating System; vulnerability identification numbers and descriptions; and software version numbers. This information is used for auditing, compliance, and vulnerability mitigation, and facilitates hardware asset management (HWAM), vulnerability management, and compliance management. CVTM enables CDC to meet Health and Human Services (HHS) and The Federal Information Security Management Act of 2002 (FISMA) requirements for continuous monitoring as mandated by Office of Management and Budget (OMB). Users are authenticated via Active Directory, a separate system with its own Privacy Impact Assessment (PIA). User id's and names are stored in one of the tools within CVTM. This information is stored with logs and not used by tool.
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 websites are used internally by the CVTM team to perform and generate scan reports from the different tools; https://acdc-sec-sc.cdc.gov http://icdc-sec-aanval.cdc.gov https://acdc-sec-apsc01.cdc.gov/ase/FolderExplorer.aspx http://icdc-sec-splunk-nwforwarder.cdc.gov https://icdc-sec-cms1.cdc.gov/login https://198.246.117.251:3000/login/login https://icdc-sec-hx:3000/login/login https://icdc-sec-mas.cdc.gov/login/login https://icdc-sec-bri-cmc https://icdc-sec-ax-cham https://ssc.cdc.gov – (User Access) https://WebInspect.cdc.gov https://apigwint.cdc.gov:9443/ https://inputs1.cdc.splunkcloudc.com https://inputs2.cdc.splunkcloudc.com https://inputs3.cdc.splunkcloudc.com https://inputs4.cdc.splunkcloudc.com https://inputs5.cdc.splunkcloudc.com https://inputs6.cdc.splunkcloudc.com https://inputs7.cdc.splunkcloudc.com https://inputs8.cdc.splunkcloudc.com https://inputs9.cdc.splunkcloudc.com https://inputs10.cdc.splunkcloudc.com https://inputs11.cdc.splunkcloudc.com https://inputs12.cdc.splunkcloudc.com https://inputs13.cdc.splunkcloudc.com https://inputs14.cdc.splunkcloudc.com https://inputs15.cdc.splunkcloudc.com https://cdc.splunkcloudgc.com https://es.cdc.splunkcloudgc.com https://idm.cdc.splunkcloudgc.com
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.	Name User Credentials
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?	The system doesn't use Personal Identifiable Information (PII).
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.	N/A. The SSN (if present) is not specifically required nor requested, but rather is incidentally collected.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Executive Order (E.O) 9397
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.	Record retrieval is through CDC Active directory and Personal Identity Verification (PIV). Which are separate systems with an approve PIA.

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.	N/A
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
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.	The information is not collected from the general 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.	The system does not solicit information directly from individuals and simply collects the information made available by them. If an individual provides information under such circumstances, he or she would be voluntarily providing it; the option is to not connect to the CDC network, once they have read the system use notification.
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 Process in Place. Individuals do not have an opportunity to consent to a particular use of the data collected because the system does not directly solicit any information from the individual.
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.	No Process in Place. The system does not solicit information directly from individuals and simply collects the information made available by them.

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 Process in Place. 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.
PIA - 17:	Identify who will have access to the PII in the system.	Users 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.	Users - Information Security Analysts for malware investigation and logs review. Administrators - System Administrators grant access to Security Analyst
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Per a role-based access model, system administrators of the Cybersecurity Program Office (CSPO) Incident and Response team are required to grant access to analyst for Office of Safety, Security, and Asset Management (OSSAM) during the on-boarding process to ensure the individual requesting access has a need to know. Information Security Analysts can then access the information and resources that are necessary for their role (role-based access) in conducting forensic analysis and support.
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.	Authorized Information Security Analysts are given access to tools with limited network visibility, and therefore limited potential access to PII. With least privilege in place, analysts only review relevant portions of traffic pertaining to their investigation.
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 must take Annual Security and Privacy Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All system users must complete the role-based-training course: “HHS Information Security for IT Administrator.

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).	A computer incident within the Federal Government as defined by NIST Special Publication 800-61, Computer Security Incident Handling Guide, Revision 2, (August 2012) is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. This item covers records relating to attempted or actual system security breaches, including break-ins ("hacks," including virus attacks), improper staff usage, failure of security provisions or procedure and potentially compromised information assets. Information is destroyed 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use. 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- CSPO Incident Response team and Security Analyst have access to the system, with Training. Technical- System is located behind a Firewall Physical- Access to the system is secured via ID badges and locked doors.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	3/25/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: March 25, 2024	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	3/28/2024
		SOP Days Open:	7

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	4/17/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski 4/16/2024: Per discussion with CDC we're including this note for updates to the next iteration of the PTA: *CVTM does not collect PII except for user credentials. However, due to the nature of the tools, which ingest data from CDC systems (e.g., system logs) there is potential PII to be inadvertently collected. This PII would be covered in the PIA for its source system.* With comments being address by the above statement, this PIA is ready for SAOP review and approval. 3/20/2024: Please see the comments and update accordingly: PTA--5A and PTA-8: The reviewer notes that PTA-5A and PTA-8 did not sync. PIA-1: Please spell out "PHI" on first use. PIA-6A: Even if incidentally collected you have to provide a legal authority. Please include "E.O.9397" in your response.	**Agency Privacy Analyst Days Open:**	20

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Signature.docx
SAOP Comments:	Approved on behalf of Bridget Guenther	**SAOP Review Date:**	4/17/2024
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CVTM Privacy_Impact_Assessment_PIA_bl (response).rtf	940230	.rtf	4/10/2024 9:53 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 4	Data Feed Service, piafrmcdc	3/15/2024	Why is it found in the scan logs?	
PIA - 1	LASKOWSKI, JAMES	3/20/2024	The reviewer notes that PTA-5A and PTA-8 did not sync.	
PIA - 6A	BLAND, CRYSTAL	3/20/2024	Even if incidentally collected you have to provide a legal authority. Please include "E.O.9397" in your response.	
PIA - 1	BLAND, CRYSTAL	3/20/2024	Please spell out "PHI" on first use.	
PIA - 1	Data Feed Service, piafrmcdc	3/28/2024	NA	
PIA - 1	BLAND, CRYSTAL	4/17/2024	On the next iteration of the PTA please include the following language in PTAa-5 response: *"CVTM does not collect PII except for user credentials. However, due to the nature of the tools, which ingest data from CDC systems (e.g., system logs) there is potential PII to be inadvertently collected. This PII would be covered in the PIA for its source system."*	

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:	4/17/2024 8:02 PM	**History Log:**	View History Log