Privacy Impact Assessment (PIA): CDC - CCFL - QTR4 - 2023 - CDC7058825

Created Date: 4/29/2024 4:01 PM Last Updated: 6/4/2024 12:01 AM

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 - CCFL - QTR4 - 2023 - CDC7058825	**PIA ID:**	1816830
Name of Component:	CDC - CSPO Cyber Forensic Lab Infrastructure	**Name of ATO Boundary:**	CSPO Cyber Forensic Lab Infrastructure
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	214
Submission Status:	Re-Submitted	**Submit Date:**	5/14/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC7058825
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.	5/29/2024
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 new changes
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.	Cybersecurity Program Office (CSPO) Cyber Forensic Lab (CCFL) Infrastructure uses a network based product that allows remote computer forensic analysis and support for all systems on the CDC network. It also provides remote imaging capability and e-discovery for legal hold requirements. CCFL also identifies malicious processes running in Random Access Memory (RAM).

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.	Forensic information is collected as needed for investigations. The type of PII collected pertaining to the forensic support and analysis varies and can not be limited to a specific categories such as: Name Driver's License Number Phone Numbers Mailing Address Education Records User ID/password related to CDC employees or contractors.
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.	CSPO Cyber Forensic Lab (CCFL) Infrastructure uses a network based product that allows remote computer forensic analysis and support for all systems on the CDC network. It also provides remote imaging capability and e-discovery for legal hold requirements. CCFL also identifies malicious processes running in Random Access Memory (RAM). CSPO Cyber Forensic Lab (CCFL) collects security controls information, system configuration files, log files, forensic data, and vulnerability status information. CCFL does not specifically target or store PII; however, PII may be inadvertently collected during forensics analysis and support. CCFL collects limited POC name, phone number, mailing address, education record, drivers license information, and user ID/password related to CDC employees or contractors. Forensic tools on this system may extract malicious files out of stored network traffic or from system memory captured from another CDC system. These files are deleted from the system as soon as the associated malware investigation is completed.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	
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.	Name Phone numbers Education Records Mailing Address User Credentials 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?	CSPO Cyber Forensic Lab (CCFL) Infrastructure uses a network based product that allows remote computer forensic analysis and support for all systems on the CDC network. It also provides remote imaging capability and e-discovery for legal hold requirements. CCFL also identifies malicious processes running in Random Access Memory (RAM). CSPO Cyber Forensic Lab (CCFL) collects security controls information, system configuration files, log files, forensic data, and vulnerability status information. CCFL does not specifically target or store PII; however, PII may be inadvertently collected during forensics analysis and support. CCFL collects limited POC name, phone number, mailing address, education record, drivers license information, and user ID/password related to CDC employees or contractors. Forensic tools on this system may extract malicious files out of stored network traffic or from system memory captured from another CDC system. These files are deleted from the system as soon as the associated malware investigation is completed.
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 Collected
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable
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.	Directly from an individual about whom the information pertains Email Government Sources Within the OPDIV Other HHS OPDIV Foreign
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.	Under the Privacy Reduction Act (PRA), “the public” includes individuals, partnerships, corporations, universities, nonprofit organizations, State, local, and tribal governments and agencies, and other associations and organizations, whether foreign or domestic. CCFL 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.	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 PII is specifically collected or used through the use of the system, except in the case of CCFL forensics. CCFL includes server-based tool for forensic analysis of electronically stored information consisting of email addresses. 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 csirt@cdc.gov or by phone 866-655-2245.
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 by the System Administrator, 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.	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 CCFL Administrator has access to PII (user name, user ID) for the purpose of creating user accounts.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access is granted during on boarding by Management using the Role Based Access model (RBAC) for the Forensics Team. Only CFL Administrators are granted access to view information related to their job duties in 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.	Administrators only have access needed to perform job functions utilizing least privilege. This limits their access to data only pertaining to their analysis.
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 at least 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 Role Based Access Controls based on Active Directory (AD) permissions. Non-repudiation through the support of digital signatures and encrypted email using Personal Identity Verification (PIV) card. Physical Controlled physical access within data centers and monitored access to components. Emergency shutoff systems. Fire and water damage protections.

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:**	5/17/2024
		SOP Days Open:	3

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 5/23/2024 Per CDC email (see supporting Documentation), confirm that PTA-7A response is Yes as it did not sync to OIS, This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	6

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per CDC email (see supporting Documentation), confirm that PTA-7A response is Yes as it did not sync to OIS.	**SAOP Review Date:**	6/3/2024
		SAOP Days Open:	11

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Copy_of_CCFL Privacy_Impact_Assessment_PIA_bl (7).rtf	203851	.rtf	5/23/2024 3:41 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	4/29/2024	Selected "user credentials"	
PIA - 14	Data Feed Service, piafrmcdc	5/13/2024	PIA-9 states PII is received directly from the individual via email. Please clarify.	
PIA - 1	BLAND, CRYSTAL	5/23/2024	Reviewer notes that PTA-5A and PTA-5B did not sync to OIS.	

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:	6/4/2024 12:01 AM	**History Log:**	View History Log