Privacy Impact Assessment (PIA): CDC - CETP - QTR2 - 2025 - CDC8727228

Created Date: 8/4/2025 8:01 PM Last Updated: 9/17/2025 4:01 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 - CETP - QTR2 - 2025 - CDC8727228	**PIA ID:**	3599659
Name of Component:	CDC - CSPO Email Threat Prevention	**Name of ATO Boundary:**	CSPO Email Threat Prevention
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	98
Submission Status:	Re-Submitted	**Submit Date:**	9/10/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8727228
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.	8/4/2025
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

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 in 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 Cybersecurity Program Office Email Threat Prevention (CETP) platform is a Cybersecurity Program Office (CSPO) managed system that serves as the primary electronic mail (e-mail) security gateway for all messages sent from external entities to CDC personnel. Messages and/or e-mail attachments deemed suspicious/malicious after inspection are quarantined immediately and made available to Cybersecurity Program Office (CSPO) cyber investigative staff for further examination. CDC is using the auto-remediation feature in FireEye ETP. This feature allow FireEye ETP to access the CDC Office 365 tenant to remove and quarantine messages that have been identified as a threat after the message was delivered to the CDC recipients. CSPO Engineers can also use the FireEye ETP message tracking to search for specific messages then use the manual remediate button to remove the message from the mailbox and place into the FireEye Quarantine.
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.	CETP leverages advanced threat detection inspects outgoing messages from external entities. Messages and/or e-mail attachments deemed suspicious/malicious after inspection are quarantined immediately and made available to Cyber Security Program Office (CPO) cyber investigative staff for further examination. They include name and email address. Users are authenticated using multi-factor authentication, using a one time password (soft token), user id, and password. Log in credentials are not stored.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Username Password Non-HHS User Credentials Username Password Email Address
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.	The Cybersecurity Program Office Email Threat Prevention (CETP) platform is a Cybersecurity Program Office (CPO) managed system that serves as the primary electronic mail (e-mail) security gateway for all messages sent from external entities to CDC personnel. They include name and email address. CETP leverages advanced threat detection inspects outgoing messages from external entities. Messages and/or e-mail attachments deemed suspicious/malicious after inspection are quarantined immediately and made available to Cybersecurity Program Office (CPO) cyber investigative staff for further examination. Users are authenticated via USER ID & password. No data is stored.

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?	
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 Cybersecurity Program Office Email Threat Prevention (CETP) platform is a Cybersecurity Program Office (CPO) managed system that serves as the primary electronic mail (e-mail) security gateway for all messages sent from external entities to CDC personnel. CETP leverages advanced threat detection capabilities coupled with up-to-the-minute threat intelligence to inspect all e-mail messages destined for CDC. Messages and/or e-mail attachments deemed suspicious/malicious after inspection are quarantined immediately and made available to Cybersecurity Program Office (CPO) cyber investigative staff for further examination. CETP is also one of only three platforms that integrate seamlessly with the Department of Homeland Security (DHS) Intrusion Prevention Security Service (IPSS). CETP also integrates directly with Microsoft Office 365, which reduces the number of “hops” e-mail must traverse before delivery to CDC personnel. CDC is using the auto-remediation feature in Trellix FireEye ETP. This feature allows Trellix FireEye ETP to access the CDC Office 365 tenant to remove and quarantine messages that have been identified as a threat after the message was delivered to the CDC recipients. CSPO Engineers can also use the Trellix FireEye ETP message tracking to search for specific messages then use the manual remediate button to remove the message from the mailbox and place into the Trellix FireEye Quarantine.
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?	Yes
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?	Yes

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address
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?	CETP inspects Messages and/or e-mail attachments for suspicious/malicious activity.
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.	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 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.	N/A Under the PRA, Federal agencies are not included in the definition of 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 chooses to provide 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.	Due to the nature of this system there is no process in place. This tool is used to inspect incoming emails for malware or malicious activity. This system does not solicit information directly from individuals and simply collects the information made available by them, therefore no process exists.

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.	Due to the nature of this system there is 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. This system collects information in real time and PII is collected at the time of suspected malware/malicious activity therefore, no periodic review is in place.
PIA - 17:	Identify who will have access to the PII in the system.	Users
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.	Cyber investigative staff for further examination of malicious activity.
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 Incident and Response team are required to grant access to analyst for CETP during the on-boarding process to ensure the individual requesting access has a need to know. Security Analysts can then access the resources necessary for their role (role-based access) in conducting examinations of suspicious activity.
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.	Analysts access only the information and resources that are necessary for their job function (role-based access) in conducting forensic investigations. 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.	Annual Security and Privacy Awareness Training
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All other security–oriented personnel must complete the role-based-training course: “HHS Information Security for IT Administrator" annually.

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: access is only available by Analysts for there legitimate purpose (role-based access) for conducting investigative activities. Technical: This system is located behind a Firewall. Physical: This system can only be physically accessed by secured ID badges behind locked doors.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	9/11/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Bevery Walker	**SOP Review Date:**	9/11/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	9/16/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 9-15-2025 Per CDC email an attached PIA the AI comment was addressed and AI statement was added. PTA-4: *The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.* AI-based classifiers automatically evaluate sender reputation, content anomalies, and behavioral patterns to make dynamic decisions; blocking malicious emails before they reach the CDC user. The platform adapts to evolving threat vectors and supports continuous risk reduction by learning from threat intelligence feeds and prior detection outcomes. PTA-8 and PTA-11A, the response for both is "No". 9/9/2025 Please see comments and update accordingly. PTA-4: Per PTA-21, the system use AI technology. Please describe, to the best of your ability, any known AI use cases and the type of AI Technology use.. Please include the following AI statement in your response "*The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.*" PTA: The responses for the following questions did not sync on the PTA, please provide the responses for PTA-8 and PTA-11A.	**Agency Privacy Analyst Days Open:**	5

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	SAOP signature.docx
SAOP Comments:		**SAOP Review Date:**	9/17/2025
		SAOP Days Open:	1

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
9-11-2025 CDC EMAIL_Re_ HHS CDC PIA Return with Comments.pdf	237587	.pdf	9/15/2025 12:21 PM	0
CETP_PIA_bl.pdf	316621	.pdf	9/16/2025 6:53 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 22	Data Feed Service, piafrmcdc	8/4/2025	Added frequency.	
PIA - 10C	Data Feed Service, piafrmcdc	9/4/2025	Provide an explanation.	
PIA - 1	BLAND, CRYSTAL	9/9/2025	PTA-4: Per PTA-21, the system use AI technology. Please describe, to the best of your ability, any known AI use cases and the type of AI Technology use.. Please include the following AI statement in your response "*The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.*"	
PIA - 1	BLAND, CRYSTAL	9/9/2025	The responses for the following questions did sync on the PTA, please provide the responses for PTA-8 and PTA-11A.	

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:	9/17/2025 4:01 PM	**History Log:**	**View History Log**