

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 - ESCII - QTR2 - 2024 - CDC8086132	PIA ID:	1800975
Name of Component:	CDC - Enterprise Systems Catalog	Name of ATO Boundary:	Enterprise Systems Catalog
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	97
Submission Status:	Submitted	Submit Date:	4/3/2024
Next Assessment Date:	N/A	Expiration Date:	1/1/2100
Office:		OPDIV:	CDC
Security Categorization:		OpDiv PIA ID:	CDC8086132
Legacy PIA ID:		Make PIA available to Public?:	Yes
1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Disposition	
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.	4/30/2024	
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.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	None.
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 Enterprise Systems Catalog (ESCII) is a web-based application used by the Enterprise Information Technology (IT) Portfolio Office (EITPO) to track all active CDC IT investments. This repository allows CDC to accurately report and respond to the Department of Health and Human Services (HHS) and Office of Management and Budget (OMB) data calls, and categorize IT spending. Additionally, ESCII serves as an inventory system of CDC applications and 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.	<p>The system inventories application/system level contact information such as names of Business Steward(s), Technical Steward(s), Security Steward(s) and their CDC phone numbers. Each application/system entry within ESCII contains information about whether the system contains PII; Authority to Operate status; server hosting status; PIA status. The system also maintains information related to system architecture, and application financial information.</p> <p>Users are authenticated through Active Directory, thus no passwords are required. Active Directory is a separate system covered by a separate PIA.</p>
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.	<p>ESCII is an application and system inventory repository system that is used for reporting and responding to HHS and OMB data calls and allows EITPO to categorize IT spending. The system inventories application/system level information and includes contact information such as names of Business Steward(s), Technical Steward(s), Security Steward(s) and their CDC phone numbers.</p> <p>ESCII contains application/system information in regards to system architecture, application financial information such as budget year and spending for each system; Capital Planning and Investment Control (CPIC) investments; names and contact information of responsible parties associated with that particular application/system; and Authority to Operate (ATO) status. This information is collected for the purpose of allowing the Enterprise IT Portfolio Office (EITPO) to track all active CDC IT investments.</p> <p>This application collects business contact phone numbers and names. Users are authenticated through Active Directory, thus no passwords are required. Active Directory is a separate system covered by a separate PIA.</p>
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?	Yes
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 Enterprise Systems Catalog (ESCII) is a web-based application used by the Enterprise Information Technology (IT) Portfolio Office (EITPO) to track all active CDC IT investments. This repository allows CDC to accurately report and respond to the Department of Health and Human Services (HHS) and Office of Management and Budget (OMB) data calls, and categorize IT spending. Additionally, ESCII serves as an inventory system of CDC applications and systems. The website is accessed by URL for CDC employees. Users are authenticated through Active Directory, thus no passwords are required.
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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not 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 Phone numbers
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?	PII is used to provide points of contact for individual systems, who the owners are and how to contact them.
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
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.	5 USC, Section 301, Departmental operations
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 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.	N/A This system does not process from or about 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.	Contact information is required within ESC for the points of contact for a system. Once a stewardship role has been accepted there is no opt-out method.
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.	If major changes were to occur to the system, a CDC-wide electronic notice would be dispensed to alert users that the system was being updated. Candidates' data with unsuccessful in-processing will be removed from 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 Help-desk or Cybersecurity Protection Office (CSPO) if they believe their PII has been inappropriately obtained. Individuals can contact the Help Desk via phone or email listed in the 'Help' section of ESC The Help-desk phone number is 404-639-7500, and the Helpdesk email address is magichelp@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.	Administrators review records on an ongoing basis for accuracy. These records are reviewed and the user is asked to update and correct their information every time they take the foreign travel safety test.
PIA - 17:	Identify who will have access to the PII in the system.	Users 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.	Users - Users can view their own information. Direct contractors fall under this category as each user only has the ability to view their own PII. Contractors can access this system, who are classified as direct contractors. Administrators - Maintenance and updates to the system, and when changes occur, they must make the appropriate changes to point of contacts information. Contractors - Direct contractors who are users can view their own information.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to the ESC application is limited to authorized, internal CDC users with a valid CDC network account. Internal user authentication will be done through Front-End Access Method. FAME and the roles that area associated with the ESC profile. Users do not have access to any PII other than their own.

<p>PIA - 20:</p>	<p>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.</p>	<p>ESC uses FAME to manage user access to data elements. FAME is used to establish roles that limit access to ESC reports to only those reports that are required for the user to perform their job. The roles determine what data types are available to a user. FAME also uses exceptions to limit the scope of the record sets that are returned to the user based on administrative codes (identifiers for specific CDC organizational units).</p>
<p>PIA - 21:</p>	<p>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.</p>	<p>Through initial and annual security and privacy awareness training, users are instructed on their responsibilities for protecting PII and acknowledge the CDC Rules of Behavior that require user's to protect PII as a pre-condition of network access. Most often completed through the Safety Awareness Training (SAT).</p>
<p>PIA - 22:</p>	<p>Describe the training system users receive (above and beyond general security and privacy awareness training).</p>	<p>None.</p>
<p>PIA - 23:</p>	<p>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).</p>	<p>All official records are transferred or destroyed based on CDC record management policies and practices. Disposal methods include burning or shredding hard copy and erasing computer tapes and disks. The following records schedules apply to the system:</p> <p>GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records</p> <p>Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.</p>
<p>PIA - 24:</p>	<p>Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.</p>	<p>Administrative: Records are maintained according with CDC's record control schedule and record control policy. The PII is secured using the CDC/IS Active Directory authentication process and role based application control via Role-Based Access Control (RBAC).</p> <p>Technical: Monitored by the Network and IT security controls which is administered by CSPO and Digital Services (DSO) In addition, the image documentation containing PII will be encrypted using industry standard encryption algorithms.</p> <p>Physical: Controls are managed by security guards, ID badges, locked doors, and key card restrictions.</p>

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	4/8/2024
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:	5/6/2024
		SOP Days Open:	33

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	5/24/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski 7/9/2024 Per CDC, this system is migrating from a Stand-Alone Component to a Sub-Component within the ISB Infrastructure. In addition to this system having its own PTA/PIA, ISB Infrastructure will have its own approved PTA. 5/24/2024 PTA-5A and PTA-5B was blank but CDC provided the response in PTA-5. This PIA is ready for SAOP review and approval.	Agency Privacy Analyst Days Open:	18

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per CDC, this system is migrating from a Stand-Alone Component to a Sub-Component within the ISB Infrastructure. In addition to this system having its own PTA/PIA, ISB Infrastructure will have its own approved PTA. PTA-5A and PTA-5B was blank but CDC provided the response in PTA-5.	SAOP Review Date:	7/9/2024
		SAOP Days Open:	46

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
RE_ CDC - ESCII - QTR2 - 2024 - CDC8086132.pdf	901071	.pdf	6/25/2024 1:20 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	5/24/2024	Reviewer notes that PTA-5A and PTA-5B are blank, please include appropriate responses on the next iteration of the PTA.	
PIA - 1	Data Feed Service, piafrmc	9/30/2024	This System has been migrated within the OCIO ISB Infrastructure Services authorization boundary. All future updates should be made via the new Sub- Component application.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	Is OpDiv Privacy Analyst Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	Is SOP Return ?:	0
Is SAOP Approved?:	1	Is Agency Privacy Analyst Return ?:	0
Total Approved:	4	Is SAOP Return ?:	0
Total Approval Required:	4	Total Return:	0

Miscellaneous Fields

Last Updated:	9/30/2024 8:01 PM	History Log:	View History Log
---------------	-------------------	--------------	----------------------------------