

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 - WCPS - QTR1 - 2024 - CDC7428034	PIA ID:	1761446
Name of Component:	CDC - Workforce Contingency Planning System	Name of ATO Boundary:	Workforce Contingency Planning System
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	38
Submission Status:	Submitted	Submit Date:	1/29/2024
Next Assessment Date:	N/A	Expiration Date:	1/1/2100
Office:		OPDIV:	CDC
Security Categorization:		OpDiv PIA ID:	CDC7428034
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.		2/29/2024
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.	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 Workforce Contingency Planning System (WCPS) is a web-based system designed to allow CDC managers to designate the furlough category for CDC staff members according to the Office of Management & Budget (OMB) criteria.

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>WCPS will collect the following CDC business information only from the Person database:</p> <ol style="list-style-type: none"> 1. Employee Name 2. User ID 3. Centers, Institutes or Offices (CIO) 4. Administrative Code 5. Occupational Series 6. Occupational Series Description 7. Work location 8. Person Category 9. Exception Reason 10. Exception Reason Modified Date 11. Grade 12. Pay Plan <p>Person Database is a Database, which is a CDC Asset; databases are not systems nor do they have PIAs. Users access this system using Active Directory (AD) which 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>WCPS provides authorized CDC managers the following functionality:</p> <ol style="list-style-type: none"> 1. Defined reports to support workforce management and planning activities associated with preparation for a possible absence of federal appropriations; 2. An automated solution to manage business rules related to furlough management; 3. Ability to document exceptions and reasons for each individual staff member at the CDC; 4. Ability to classify CDC staff members as an employee, contractor, or affiliate; and 5. Defined reports and advanced search functionality. <p>An authorized CDC management official is able to access the system and enter search criteria to view the desired result set (i.e., the staff member(s) requiring changes to the exception reason). They can then select the appropriate exception reason for the selected staff member(s) and can continue their search or filter criteria to view and/or modify the exception reason for additional staff. The CDC management official can also generate reports as needed to view the exception reason for specific staff through the CDC Enterprise Reporting System (CERS). CERS is a reporting server, that is a tool CDC uses, it is not a system on its own and has no PIA.</p> <p>The system's database, Management Information Systems Office (MISO), pulls business contact information from MISO_Person and views Administrative Codes through the MISO_AdminCodes databases. Users access this system using Active Directory; which 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 Workforce Contingency Planning System (WCPS) is a web-based system designed to allow CDC managers to designate the furlough category for CDC staff members according to the Office of Management & Budget (OMB) criteria. CDC Users access WCPS through the URL (https://wcps.cdc.gov).
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?	
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 Employment Status 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?	An authorized CDC management official is able to access the system and enter search criteria to view the desired result set (i.e., the staff member(s) requiring changes to the exception reason). They require employee name or User ID in order to identify the correct employees for changes to the exception reason. They can then select the appropriate exception reason for the selected staff member(s) and can continue their search or filter criteria to view and/or modify the exception reason for additional staff.
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 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Employee name or User ID
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.	OPM GOVT-1 General Personnel Records
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.	Individuals provide their PII as a condition of being considered for a position within the CDC. Individuals can only opt out by refusing, or deciding, not to send CDC or its affiliates their application for employment. Users consent to supply their information when they request to be considered for a position. There is no opt-out as it is a condition of employment.
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. Managers would push out notice's that the purpose of the system was changing.
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 Technical Service Branch (TSB) Help-desk or Cybersecurity Program Office (CSPO) if they believe their PII has been inappropriately obtained, used or disclosed or is inaccurate. Individuals may contact the Help Desk via phone or email listed in the 'Help' section of WCPS. 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 his or her information every time he or she takes the foreign travel safety test.
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 - Users can view their own information for the purposes of tracking their furlough status and information. There are no contractors as part of this system, as furlough only applies to full time employees. Administrators - Managers can view PII to allow them to designate the furlough category for CDC staff members according to the Office of Management & Budget (OMB) criteria

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	A user's access to PII is enforced via role based access control. Permissions are assigned to WCPS roles, and users are assigned to roles with the lowest level of permissions necessary to complete their job. The WCPS Product Owner is the authorized approver for WCPS roles. All role requests must originate or be approved by the WCPS Product Owner or designated representative. Upon verification of approval, the role requests will then be routed to the System Administrators, who will assign users to those roles.
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.	WCPS uses Front-end Access Method (FAME)(ME= Method) to manage user access to data elements. FAME is used to establish roles that limit access to WCPS 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).
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.	Users are instructed on their responsibilities for protecting PII through initial and annual security and privacy awareness training (SAT).
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	None.
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).	<p>All official records are transferred or destroyed based on CDC record management policies and practices. The following records schedule applies 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>
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.	<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 RBAC.</p> <p>Technical: Monitored by the Network and IT security controls. 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:	1/30/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: January 30, 2024	Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	2/5/2024
		SOP Days Open:	7

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	2/6/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski 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:	24

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	1/30/2024	Please select "user credentials" and "employment status"	
PIA - 1	LASKOWSKI, JAMES	2/6/2024	The reviewer notes that PTA-12 did not sync.	
PIA - 1	BLAND, CRYSTAL	2/6/2024	FOr update on the next iteration of the PTA: PTA-5A: Please select "Yes, but user credentials are maintain by another system..."	
PIA - 1	Data Feed Service, piafrmcdc	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
---------------	-------------------	--------------	----------------------------------