Privacy Impact Assessment (PIA): CDC - BAS - QTR2 - 2024 - CDC8208361

Created Date: 5/6/2024 4:01 PM Last Updated: 6/20/2024 8:01 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 - BAS - QTR2 - 2024 - CDC8208361	**PIA ID:**	1821743
Name of Component:	CDC - Building Automation System	**Name of ATO Boundary:**	Building Automation System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	50
Submission Status:	Re-Submitted	**Submit Date:**	5/28/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	High	**OpDiv PIA ID:**	CDC8208361
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.	5/31/2024
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.	Not Applicable
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 CDC Building Automation System (BAS) is a Direct Digital Control system (DDC) made of several parts which consist of: 1) field level controllers with attached sensors, relays, valve actuators, damper actuators and etc. 2) supervisory controllers 3) servers and 4) workstations. The DDC system provides automated processes for running and operating Heating Ventilation and Air Conditioning (HVAC) equipment and allows the maintenance operators, technicians and engineers to monitor and operate systems and spaces based on their password level which is set by either the Campus BAS Controls Engineer, BAS Lead Electronics Technician or the Senior Electronic Technician for the building being monitored. The BAS provides the following services to the CDC: 1. Campus chilled water distribution; 2. Steam conversion and hot water distribution; 3. Indoor air quality; 4. Air flow distribution into the spaces; 5. Lab containment control BSL1 and 2; 6. Lab containment control BSL 3; 7. Lab containment control BSL 3+/4 building 18; 8. Freezer/Refrigerator/Incubator monitoring; 9. Utility monitoring; 10. Energy 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.	The BAS system collects analog and binary hardware point trend and alarm data associated with CDC mechanical systems (including the BAS itself) for the purposes of monitoring those systems performance and diagnosing system issues. BAS is collecting hardware/sensor data installed and is programmed into the BAS controllers and system applications. The BAS application audit data is also collected on user initiated changes, such as baseline configurations. This data is collected by the system by default. Additionally, BAS collects authentication information such as user ID/user name and user password; work email and phone; timestamps; and classification of the action. User ID and passwords are stored temporarily for 2 years.
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 Email Address HHS Username Password

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.	BAS collects trend and alarm data associated with CDC mechanical systems for the purpose of monitoring the buildings and systems for proper operation as configured and programmed by authorized users. Audit log data (modifications of set points and loads, and/or utility rates) is logged automatically to record user changes to the system. For user accounts, BAS stores CDC UserID, CDC email address and CDC Phone. User IDs/name and passwords are used for authentication. Timestamps, and classification of the action are used for audit logs to record user activity (information system security). User ID and passwords are stored temporarily for 2 years.
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?	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)?	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.	
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?	Yes
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 Email Address Phone numbers 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.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	Primary use of PII is to authenticate system login.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	PII is also used to record user activity for audit logs.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	N/A - the system does not collect, store or maintain SSNs.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	N/A - the system does not collect, store or maintain SSNs.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC 301
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 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.	Users are required to provide their PII prior to gaining access to BAS; it is required to set up an account.

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.	There is no method to opt out of the collection or use of their user PII if individuals are requesting access to the BAS system.
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.	There is no process in place to notify and obtain consent from individuals whose PII is in the system. Major changes that will require a materially different use of the PII is not anticipated.
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.	Users can contact the System Owner or the Office of Safety, Security and Asset Management (OSSAM) Information System Security Officer (ISSO) via phone or email (i.e. ossamisso@cdc.gov) with concerns when they believe their PII has been inappropriately obtained, used or inaccurate.
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.	User Audits are performed quarterly for periodic reviews of PII contained in the system. There is an entitlement review performed for all users quarterly. This review determines availability and if the user is still in need the level of access or overall access to the system. Since the information is taken directly from the user, integrity and accuracy would be individually validated .
PIA - 17:	Identify who will have access to the PII in the system.	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.	Administrators - Administrators will have access to PII to review audit logs. Contractors - There are also a limited number of direct contractor(s) who have access to PII to perform review of audit logs.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrators and Contractors (each limited to the functions and information which is essential to their job functions) are the only users that have access to PII. The system administrators are required to complete a User Permission Request Form prior to access to the system and PII. This form is then approved by system owner once confirmation of proper training and background approval.
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 and Contractors are the only users who have access to PII. The administrative users are limited to individuals that have been approved by the system owner using the security control principle of least privilege. The administrators are authorized by role based access (BAS system administrators). This role base access limits unauthorized users from PII information.
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.	CDC requires 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).	Certain users are also required to undergo Role Based Training.
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).	OSSAM performs database purges pursuant to the Engineering Maintenance Operation Service (EMOSO) Data Retention Standard Operating Procedure (SOP) (purge all database data older than 2 years old). OSSAM also performs backup purges from Share Drives and Network Attached Storage (NAS) drives pursuant to the EMOSO Data Retention SOP (purge all backups older than 36 months unless marked to be kept indefinitely). Records Retention Schedules applicable to BAS are: DAA-GRS¬2013-0002¬0016 Tracking and control records when no longer needed DAA-GRS¬2013-0002¬0007 Record management program records destroyed after 6 years DAA-GRS¬2013-0002¬0008 Vital or essential record program records destroyed after 3 years DAA-GRS¬2013-0002¬0015 Copies of vital records destroyed after the next cycle DAA-GRS¬2013-0002¬0009 Forms management records destroyed after 3 years

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: The owner of the system provides access according to their role, user roles, access policy, awareness training, privacy impact assessments, security assessments. Technical: The BAS encrypts its databases and retains data as backup zip files of those databases until we are allowed to delete those backups per the data retention policy, which can be changed at any time by Cyber Security Program Office (CSPO). Multi-factor authentication (PIV credentials, Username/ Password), Active Directory, Firewall and IDS. Physical: Guards, ID badges, Key Cards and readers, and Closed-Circuit Television (CCTV).

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/28/2024
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:**	5/28/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	6/11/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/11/2024 The comments that reference the PTA are comments for the next iteration of the PTA. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	14

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	On next iteration of PTA, please provide a response to PTA-5A.	**SAOP Review Date:**	6/20/2024
		SAOP Days Open:	9

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 19	Data Feed Service, piafrmcdc	5/23/2024	Are the direct contractors mentioned above included in the administrator category as the only people with access to PII? It's unclear.	
PIA - 20	Data Feed Service, piafrmcdc	5/23/2024	Are the direct contractors mentioned above included in the administrator category as the only people with access to PII? It's unclear.	
PIA - 23	Data Feed Service, piafrmcdc	5/23/2024	Has SOP and NAS been defined already?	
PIA - 24	Data Feed Service, piafrmcdc	5/23/2024	OCISO is now the Cyber Security Program Office.	
PIA - 1	VILLAFUERTE, NESTOR	6/10/2024	PTA-4 - If "BSL" is an acronym, please spell it out in its first instance.	
PIA - 1	BLAND, CRYSTAL	6/11/2024	On next iteration of PTA, please provide a response to PTA-5A.	

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:	6/20/2024 8:01 PM	**History Log:**	View History Log