Privacy Impact Assessment (PIA): CDC - ALTA - QTR4 - 2024 - CDC8559862

Created Date: 11/21/2024 7:01 PM Last Updated: 5/12/2025 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 - ALTA - QTR4 - 2024 - CDC8559862	**PIA ID:**	2461625
Name of Component:	CDC - Atlassian Cloud	**Name of ATO Boundary:**	Atlassian Cloud
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	179
Submission Status:	Re-Submitted	**Submit Date:**	5/1/2025
Next Assessment Date:	N/A	**Expiration Date:**	5/11/2028
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8559862
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Development
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	5/1/2025
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.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred 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 purpose of Atlassian Government Cloud is to provide product owners, project managers, and various developers with a common set of project management tools and internal documentation portal including various tooling through Jira, Confluence, and Status page. Today, various Centers host their own version of Atlassian, whether it is in the cloud or on-premises. Jira- tool for tracking, managing, and planning software development tasks Confluence- workspace for creating, organizing, and sharing knowledge and documentation Status page- communication tool to share real-time status updates and incident information with users and stakeholders

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 Atlassian system does not solicit, collect or request specific personally identifiable information (PII); however, it is expected that individuals or groups of individuals will include PII in the execution of their duties. The type of PII that the system will collect or maintain: Any information a user chooses to include such as unspecified PII. This system does not collect any personal identifiable information (PII) of the general public. It is a system of tools (ex. Jira, confluence, statuspage) of metrics for project planning and other systems. Any PII it collects are of CDC staffers (ex. CDC officials and CDC contractors), and the type of PII information are names and email addresses. As such, we do not believe that a PIA applies to Atlassian Government Cloud. Communications via Email, IM and/or various documents transmitted between CDC employees, between agency employees and employees of other federal, state and local agencies, and in some cases employees and non-government external individuals, for normal day-to-day business operations. PII is never explicitly solicited from individuals or used by the system (i.e., there are no forms or fields for PII submission, and PII collection is not the explicit purpose of the system).
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.	The Atlassian system does not solicit, collect or request specific personally identifiable information (PII); however, it is expected that individuals or groups of individuals will include PII in the execution of their duties. The type of PII that the system will collect or maintain: Any information a user chooses to include such as unspecified PII. This system does not collect any personal identifiable information (PII) of the general public. It is a system of tools (ex. Jira, confluence, statuspage) of metrics for project planning and other systems. Any PII it collects are of CDC staffers (ex. CDC officials and CDC contractors), and the type of PII information are names and email addresses. As such, we do not believe that a PIA applies to Atlassian Government Cloud. The information types identified for the system's FIPS 199 Security Categorization as documented in the Baseline System Information document include: Personal Identity and Authentication - platform access via Single Sign-On (Name, E-mail address, Active Directory credential information) Systems Development - tracking, managing, and planning software development tasks IT Infrastructure Maintenance - real-time status updates and incident information Information Sharing - creating, organizing, and sharing knowledge and documentation
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
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)?	
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 purpose of Atlassian Government Cloud is to provide product owners, project managers, and various developers with a common set of project management tools and internal documentation portal including various tooling through Jira, Confluence, and Statuspage. Access is allowed through Zscaler, Citgo, and the public Internet. However, only internal CDC personnel with approved Active Directory logins are able to sign-in to the CDC-specific Atlassian websites. All other users will be denied entry.
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?	
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	No
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 - Collect PII Persistent Cookies - 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?	

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Social Security Number Truncated SSN Name Mother Maiden Name Email Address Phone numbers Certificates Taxpayer ID Date of Birth Mailing Address Medical Records Number Financial Account Info Legal Documents Devices Identifiers Passport Number User Credentials Driver License Number Others - Chart No., TIN, DUNS, Provider License #
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) 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?	Atlassian is a system of tools (ex. Jira, confluence, status page) of metrics for project planning and other systems and the type of PII information are names, device identifiers and email addresses. Communications via Email, IM and/or various documents transmitted between CDC employees, employees of other federal, state and local agencies for normal day-to-day business operations. PII is never explicitly solicited because there are no forms or fields for PII submission but communications with PII can be included as attachments within the various Atlassian environments.
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.	SSN and/or Taxpayer ID are not used in the function of this system but users may enter them in free-text fields if there is a justifiable business need. Data stewards ensure that any PII within the environment meets required business needs.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	EO 9397
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC 301, Departmental Regulations
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.	Atlassian 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 data that is specifically collected or used throughout the use of the system is limited in scope to an end users need; therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the onboarding process for CDC employees and the underlying use of the service.
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.	The data that is specifically collected or used throughout the use of the system is limited in scope to an end users need; therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the onboarding process for CDC employees and the underlying use of the service. It is the responsibility of the program administering the business process to notify users of major changes.

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.	Atlassian has a security incident management policy that provides a structured framework for data breaches, including those involving PII. The frame work includes Detection, Investigation, Containment, Eradicate and Recovery. Once this process is completed Customer notification and Transparency is then provided with details of breach. Individuals can obtain/read the security incident management policy at Security Incident Management Process | Atlassian https://support.atlassian.com/contact/ (Atlassian does not have a number you can contact directly)
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.	Data integrity is maintained at the level of the business process, or through maintenance of the applications that support business processes. Atlassian originates from a separate information system (Jira) which has its own processes for maintaining integrity, availability, accuracy and relevancy. Periodic reviews are conducted daily to ensure potential incidents are detected quickly Atlassian has a security incident management agreement policy that provides a structured framework for data breaches, including those involving PII. The frame work includes Detection, Investigation, Containment, Eradicate and Recovery. Once this process is completed Customer notification and Transparency is then provided with details of breach. Agency-wide cybersecurity, physical security, continuing operations, training, and other measures also support data integrity and availability and system functionality. Users are responsible for the accuracy.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers 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: To send and receive content and perform duties. Administrators: CDC administrators provide support which may require performing queries related to PII. Contractors: Offsite (HHS/CDC credentialed) Cloud Service provider support personnel (system administrators) have access to PII in order to provide technical support upon CDC request. Developers: will appropriately map incoming data into the platform, perform validation checks, build ontology.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The System Stewards are able to leverage Role Based Access Controls that are built-in to the system and are used to enforce a least privileges model based on the principle of separation of duties, according to an access control matrix detailing which administrative job roles can perform job functions which might allow access to PII information.
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.	Enforcement of this access is implemented by a Role Based Access Control methodology which uses a least privileges model to determine access ability based on job roles. Other parties (system administrators, contractors, users not party to a specific communication, etc.) will not have access to content not specifically assigned to them, except as needed to perform support functions such as queries. Cloud providers in particular are not expected to have any access to the content of transmissions. System administrators with the appropriate permissions, who have signed Rules of Behavior and performed the required training, are able to access the contents of emails, for authorized purposes such as e-discovery or detection of breaches.
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 users are required to complete annual Information Security Training and Privacy Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users are provided annual training which will be completed once a year regarding the basic concepts of accessing services offered by the Atlassian cloud-based solution. CDC Administrators are required to complete annual training in Security Incident Response, Contingency Planning and Operations, and 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).	Records are retained and disposed of in accordance with the CDC Records Control Schedule. Records are maintained in agency until no longer needed or unless explicitly requested through an opt-out process by an individual, at which point they will be destroyed. Deletion privileges are limited to platform administrators. Disposal methods include erasing computer media when no longer needed. N1-442-09-1 Audits of system administrator deletions will be reviewed at least annually to validate compliance with the retention policy. This system adheres to General Record Schedule (GRS) 5.1 Common Office Records. The disposition instruction for this GRS is to destroy the data when the business use ceases.
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 CONTROLS: PII is secured within the system through the use of administrative controls in the form of mandatory security awareness and privacy training for all users; role-based training for privileged users; personnel screening as required by CDC; completion of contractual agreements and Rules of Behavior; and, in accordance with applicable CDC policies. TECHNICAL CONTROLS: Technical controls applied to ServiceNow include: continuous network/system monitoring; firewalls; Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Data Loss Prevention (DLP); multi-factor authentication. PHYSICAL CONTROLS: Physical controls include: Hosting within data centers which control and monitor physical access to the system components, including visitor control and auditing of access records; and, protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/1/2025
Privacy Analyst Comments:	PTA-5 Needs to be updated to explain the use of AI, known cases of AI, and to include the AI statement "*The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risk*." **This has been completed and added to PTA 5** PTA-12-12A: The system should clearly be configured to either collect personally identifiable information (PII) or not—there's no ambiguity allowed. If the decision is to collect PII (i.e., answering "yes"), then CDC will need to start the Tier 3 process prior to the approval of the PIA. ***The cookies used in ALTA are single session (tier 1) and do not collect PII.*** 4/16/2025 Please see comments and update accordingly: Does the system have a planned ATO date? **The planned ATO date is 5/1/2025 and is listed within the document. if you cannot see this on your end, it may be due to a sync issue** PTA-5A: Per PTA-6, the response should be "Yes, user credentials are collected but maintained by another system." **This has been updated** PTA-8A: Per URL Details, please select "Yes." **The URL is not available to the public. If a member of the public types in the URL, an access denial page will be shown. The response has been left as no.** Reviewer notes that PTA-11, PTA-12, and PTA-21 failed to sync. PTA-11: Please select "No." **updated** PTA-12: Per PTA-12A, the response should be "Yes." **updated** PTA-12A: Please confirm if Session and Persistent Cookies collects PII because it wasn't mention in PTA-5 response. **Single session that does not collect PII.** PTA-21: Please select Yes/No if the system use AI Tech. **updated** PIA-1: Device Identifiers was not mention in PTA-5, if device identifiers are collected please update the response to PTA-5 to include device identifiers. **updated**	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker. The xls file in the signature space was included unintentionally. I am unable to delete the file.	**SOP Review Date:**	5/5/2025
		SOP Days Open:	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/7/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 5/7/2025 Updates were made to PTA/PIA but not sure if they sync to the OIS instance of Archer. CDC Addressed some comment in the OpDiv PA section. 4/29/2025 Per CDC's emails, please see comments below: PTA-5 Needs to be updated to explain the use of AI, know cases of AI, and to include the AI statement "*The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risk*." PTA-12-12A: The system should clearly be configured to either collect personally identifiable information (PII) or not—there's no ambiguity allowed. If the decision is to collect PII (i.e., answering "yes"), then CDC will need to start the Tier 3 process prior to the approval of the PIA. 4/16/2025 Please see comments and update accordingly: Does the system have a planned ATO date? PTA-5A: Per PTA-6, the response should be "Yes, user credentials are collected but maintained by another system." PTA-8A: Per URL Details, please select "Yes." Reviewer notes that PTA-11, PTA-12, and PTA-21 failed to sync. PTA-11: Please select "No." PTA-12: Per PTA-12A, the response should be "Yes." PTA-12A: Please confirm if Session and Persistent Cookies collects PII because it wasn't mention in PTA-5 response. PTA-21: Please select Yes/No if the system use AI Tech. PIA-1: Device Identifiers was not mention in PTA-5, if device identifiers are collected please update the response to PTA-5 to include device identifiers.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	5/12/2025
		SAOP Days Open:	5

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
4-14-2025 EMAIL_RE_ CDC - ALTA - QTR4 - 2024 - CDC8559862.pdf	206636	.pdf	4/16/2025 9:43 AM	2
CDC ALTA_2_6_2025_PIM NV.rtf	989560	.rtf	4/14/2025 12:25 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc		Based off your statement in other, please select all PII data elements. You`ll also need to go to the privacy webpage https://intranet.cdc.gov/ocio/information-systems-security/privacy/index.html and download a new SSN Form. Fill out the document and have the business steward sign the SSN Form. Once that occurs, upload the document to this PIA and resubmit. Also, the BSI states that ALTA collects Name of User, Email Address and IP address. Please insure that these elements are documented here.	
PIA - 15	Data Feed Service, piafrmcdc		The Privacy Unit is not responsible for ALTA, therefore we ask that you remove that statement.	
PIA - 16	Data Feed Service, piafrmcdc		Your comments contradict what is stated in the BSI. This shows that Name of User, Email Address & IP address are collected within this tool and NOT AD. Therefore, please modify your response	
PIA - 17	Data Feed Service, piafrmcdc		Please include Users & Contractors	
PIA - 19	Data Feed Service, piafrmcdc		Please remove the first sentence as is better suited for PIA - 21	
PIA - 22	Data Feed Service, piafrmcdc		What`s the frequency of this training?	
PIA - 23	Data Feed Service, piafrmcdc		Please describe the retention and destruction process and list any Records Control Schedule (RCS) Job	

		Numbers or General Records Schedules (GRSs) that apply to the PII maintained in the system; and/or State if the appropriate RCS Job Number or GRS for some or all of the PII maintained in the system and that the PII should be maintained until a determination is provided. For assistance, please contact the CDC Records Management Team at records@cdc.gov . Please include your process for the retention and destruction of PII. (i.e. Records Control Schedules: DAA-0443-2012-0007-0006 or N1-443-00-002)
PIA - 15	Data Feed Service, piafrmcdc	This tool dose contact PII as per PIA-1, therefore the current answer provided is not acceptable. Please remove. 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 there is no process, state why not.
PIA - 16	Data Feed Service, piafrmcdc	You BSI indicates that this tool contains PII "Name of User, Email Address & IP address" therefore your comments are not accurate. Please specifically describe the process in place for periodic reviews of PII contained in the system, who process them and how frequent? If there is no process, state why not.
PIA - 18	Data Feed Service, piafrmcdc	Please include the reason for developers.
PIA - 23	Data Feed Service, piafrmcdc	Nonresponsive. Please describe the retention and destruction process and list any Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) that apply to the PII maintained in the system; and/or State if the appropriate RCS Job Number or GRS for some or all of the PII maintained in the system and that the PII should be maintained until a determination is provided. For assistance, please contact the CDC Records Management Team at records@cdc.gov . Please include

		your process for the retention and destruction of PII. (i.e. Records Control Schedules: DAA-0443-2012-0007-0006 or N1-443-00-002)
PIA - 15	Data Feed Service, piafrmcdc	Please include the process on how an individual can obtain/read the security incident management policy.
PIA - 16	Data Feed Service, piafrmcdc	Please include the name of the separate information system. Also, what is the frequency of periodic reviews?
PIA - 1	VILLAFUERTE, NESTOR	Does the system have a planned ATO date? Please provide a response to PTA-5a Reviewer notes that PTA-11, PTA-12, and PTA-21 failed to sync.
PIA - 1	BLAND, CRYSTAL	Updates to the PTA: PTA-5A: Per PTA-6, the response should be "Yes, user credentials are collected but maintained by another system." PTA-8A: Per URL Details, please select "Yes." PTA-11: Please select "No." PTA-12: Per PTA-12A, the response should be "Yes." PTA-12A: Please confirm if Session and Persistent Cookies collects PII because it wasn't mention in PTA-5 response. PTA-21: Please select Yes/No if the system use AI Tech.
PIA - 1	BLAND, CRYSTAL	PIA-1: Device Identifiers was not mention in PTA-5, if device identifiers are collected please update the response to PTA-5 to include device identifiers.
PIA - 1	Data Feed Service, piafrmcdc	Please check off all checkmarks within this field since PTA 5 mentions that any PII could inadvertently be entered by a user "The type of PII that the system will collect or maintain: Any information a user chooses to include such as unspecified PII. Please select all checkboxes in PIA 1. Please take a look at the previous comment above

		and follow the recommendation provided. We need a SSN form filled out since an individual's SSN could inadvertently be added to the system.
PIA - 4	Data Feed Service, piafrmcdc	Please spell out the acronym for IM and any other acronyms that have been used and not spelled out.
PIA - 6	Data Feed Service, piafrmcdc	Please remove Not applicable and indicate that SSN is collected since it has been advised to add SSN in PIA 1.
PIA - 6A	Data Feed Service, piafrmcdc	Please remove Not applicable and find an applicable SORN
PIA - 7	Data Feed Service, piafrmcdc	Please remove Not applicable and identify legal authorities, governing information use and disclosure specific to the system and program
PIA - 10C	Data Feed Service, piafrmcdc	PIA 5 indicated there may be information about the public, please update as applicable and remove every contradicting statement that says PII is not collected by this system.
PIA - 10	Data Feed Service, piafrmcdc	PIA 4 indicates that the system contains "Communications via Email, IM and/or various documents transmitted between CDC employees, between agency employees and employees of other federal, state and local agencies, and in some cases employees and non-government external individuals, for normal day-to-day business operations" If there is information about members of the public, then an Information collection request and OMB approval may be applicable. Please consult your records department for further guidance.
PIA - 9	Data Feed Service, piafrmcdc	PIA 4 indicates that the system contains "Communications via Email, IM and/or various documents transmitted between CDC employees, between agency employees and employees of other federal, state and local agencies, and in some cases employees and non-government external individuals, for normal day-to-day business operations"

		If there is information about members of the public, please update as applicable.
PIA - 18	Data Feed Service, piafrmcdc	Do developers have access to the system? if yes please include
PIA - 17	Data Feed Service, piafrmcdc	Do developers have access to the system. If yes please include them
PIA - 15	Data Feed Service, piafrmcdc	Please provide the contact information and refrain from using an individual`s PII and only provide group email and/or phone numbers.
PIA - 1	BLAND, CRYSTAL	Per CDC Email, Does Session and Persistent Cookies collect PII? Atlassian session and persistent cookies do not collect PII by default. They are primarily used for authentication, user preferences, and performance tracking. However, depending on the system configuration (SSO), cookies may be indirectly associated with PII. I believe that's why we were instructed to select "collect PII" as shown. Does the system use AI Technology? If so, what are the known use cases for the AI Tech? Currently Atlassian uses AI through Atlassian Intelligence which is used to enhance productivity, accelerate workflows, and streamline task for project management team.

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:	5/12/2025 4:01 PM	**History Log:**	View History Log