PTA / PIA: CDC - OCIO Azure GSS - QTR2 - 2026 - CDC8909080

Created Date: 5/21/2026 1:21 PM Last Updated: 5/30/2026 5:20 AM

General Information

PTA / PIA Name:	CDC - OCIO Azure GSS - QTR2 - 2026 - CDC8909080	**PTA / PIA ID:**	4506545
Component Name:	CDC - OCIO Azure GSS	**ATO Boundary Name:**	OCIO Azure GSS
Overall Status:	Complete	**# of Days - Open:**	16
Submitter:		**Submit Date:**	5/20/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
Office:		**OpDiv:**	CDC
Security Categorization:	High		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Barton Day
PTA 01A:	POC Title and Organization	IT Program Manager - OCOO\OCIO\DSO\CSB
PTA 01B:	POC Email Address	OSR9@cdc.gov
PTA 01C:	POC Phone Number	(404) 718-7247
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	None
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Contractor

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The purpose of Office of Chief Information Officer (OCIO) Azure General Support System (GSS) system is to acquire and provide remote cloud infrastructure resources from Microsoft Azure Services. This allows the Digital Services Office (DSO) to provide Center for Disease Control and Prevention (CDC) cloud service offerings along with current services offerings to CDC customers. Microsoft Azure has Federal Risk and Authorization Management Program (FedRAMP) authority to operate a Health & Human Services (HHS) Authorization to Operate (ATO). The OCIO Azure GSS system does not collect, maintain or share user credentials. The OCIO Azure GSS relies on Active Directory user IDs, Personal Identity Verification (PIV) smart cards, and Alternate Personal Identity Verification (ALT) smart cards for access but authentication credentials are not stored as part of the OCIO Azure GSS. The Infrastructure Services Branch hosts the customers' applications but does not own the data or have control over the use of the data in these systems.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The system will contain Life cycle/Change Management, System Maintenance, and Information Technology (IT) Infrastructure Maintenance Information in support of the Infrastructure Services Branch managed systems hosted within the cloud providers environment. The type of data would include Name, Date of Birth, Driver's License Number Mother's Maiden Name E-mail Address, Home Address, Phone Numbers, Medical Notes Financial Account Info, Education, Military Status and Employment Status. The data will be stored temporarily. The OCIO Azure GSS system does not collect, maintain or share user credentials. The OCIO Azure GSS system relies on Active Directory user IDs, Personal Identity Verification smart cards, and Alternate Personal Identity Verification smart cards for access but authentication credentials are not stored as part of the OCIO Azure GSS system. The Infrastructure Services Branch hosts the customers applications but does not own the data or have control over the use of the data in these systems internal users will use their CDC Active Directory credentials to access the system which are stored temporarily.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	CDC Active Directory
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The OCIO Azure General Support Systems GSS system will contain Life cycle/Change Management, System Maintenance, and IT Infrastructure Maintenance Information in support of The Infrastructure Services Branch managed systems hosted within the cloud providers environment. The type of data would include Name, Date of Birth, Driver's License Number

Mother's Maiden Name E-mail Address, Home Address, Phone Numbers, Medical Notes Financial Account Info, Education, Military Status and Employment Status. This data is used for research/analysis and to build cohorts for data analysis but will not be used to query on or for individuals. For example, fields like DOB will be used to derive an Age value which will be used to bucket employees into age bracket for analysis on the group. Data will be stored temporarily. The OCIO Azure GSS system does not collect, maintain or share user credentials. The OCIO Azure GSS relies on Active Directory user IDs, Personal Identity Verification smart cards, and Alternate Personal Identity Verification smart cards for access but authentication credentials are not stored as part of the OCIO Azure GSS system. Azure Government is a government-community cloud that offers hyper-scale compute, storage, networking, and identity management services, with world-class security. A physically and network-isolated instance of Microsoft Azure, operated by screened U.S. citizens, Azure Government provides standards-compliant Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) that has now received a Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authorization to Operate (ATO). All services are available immediately to support secure US government workloads, including Criminal Justice Information Services (CJIS), Internal Revenue Services (IRS) Publication 1075 Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Department of Defense (DOD), and federal agency data. Some Infrastructure Services Branch data elements would be: Splunk Agents provide for the Office of the Chief Information Officer (OCISO) continuous monitoring, System logs for system activity to be forwarded to OCISO Splunk. This is a hosting environment. Any data being hosted would be governed under the individual hosted system's Authorization to Operate and Privacy Impact Analysis for that given system.

Azure Government infrastructure has also achieved a Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authorization to Operate (ATO) supporting in-scope services, including Azure Active Directory.

In addition, the Azure public cloud platform had previously received a Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authorization to Operate (ATO), enabling government agencies and partners to deploy moderately sensitive data to the cloud. Customers can choose either compliant environment to best meet their needs for security and isolation, with assurance that control requirements are being met by comprehensive continuous monitoring and a standardized approach to risk management in both

		the public and government-community clouds. For additional information, visit the Microsoft Compliance blog and Azure Trust Center, or refer to Azure Federal Risk and Authorization Management Program (FedRAMP) Package ID# F1209051525. The following services are Federal Risk and Authorization Management Program (FedRAMP) authorized and approved by the Joint Authorization Board (JAB): KeyVault, ExpressRoute, WebApps, Azure Site Recovery (ASR), Microsoft Azure Backup (MAB), Notification Hubs, Service Bus, StorSimple, Automation, Azure Resource Manager (ARM), Batch, Media Services, Policy Administration Services (PAS), Scheduler, Log Analytics, and Redis Cache. Some Infrastructure Services Branch data elements would be: Splunk Agents to provide for the Office of the Chief Information Officer (OCISO) continuous monitoring, System logs for system activity to be forwarded to OCISO Splunk. This is a hosting environment. Any data being hosted would be governed under the individual hosted system's Authorization to Operate and Privacy Impact Analysis for that given system.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Driver's License Number Financial Account Information (e.g., account numbers, credit card numbers) Biographical Information Name Date of Birth Mother Maiden Name Education Records Employment Status/History Military Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Medical Information Medical Records Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	Citizenship Race Ethnicity County of Usual Residence State of Usual Residence Marital Status Sex HRO/Staff Data Elements: Salary, Benefits Elections, Step/Level
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Patients Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	Given the dynamic nature of this platform system, it is understood that the purpose for which PII may be processed cannot be exhaustively anticipated. Component systems within this platform system can vary in their functionality and use cases and will have their own PIA describing their specific PII use purposes.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	None.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Modernizing Government Technology Act of 2017
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes

PIA 29A:	Please specify which PII data elements are used to retrieve records.	Some component systems may and those PII data elements will be described in the component's PIA in which it applies.
PIA 29B:	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 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV State/Local/Tribal
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB 0920-0017 11/30/2028
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	As it relates to non-employees, component PIAs will address their methods in their associated PIA. Employees provide PII as a condition of employment to the CDC. Individuals can only opt-out of PII collection by not accepting employment at the CDC. Users consent to provide their information when they voluntarily register online within upstream Navigator web-application notifying users that their personal information is being collected.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	For applicable individuals, data notification and consent are handled by the component system collecting said data (each has its own PIA). For any individual who wishes to know if a system contains records about them that individual should submit a notification request to the applicable System Manager of the applicable SORN. The request must contain the same information required for an access request and must include verification of the requester's identity in the same manner required for an access request. For employees, a CDC-wide announcement would be made through a newsletter, supervisor briefings, or via an Office of the Director announcement.

PIA 36:	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.	If individuals believe their PII has been inappropriately obtained, used, or disclosed, they may contact the Help Desk, or Cyber Security Program Office (CSPO) directly with any concerns regarding their PII. Individuals can contact the Help Desk via phone or email listed in the 'Help' section of Navigator system. The Help-desk phone number is 404-639-7500, and the Helpdesk email address is magichelp@cdc.gov.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The integrity, availability, accuracy and relevancy of the data is ensured because the administrators (whose PII is contained in the system) are charged with reviewing, monitoring and ensuring that new accounts are setup and terminated as necessary. As a result, outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system.
PIA 38:	Identify who will have access to the PII in the system.	Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Administrators - Perform managerial and supervisory activities for personnel. Developers - To develop cohorts for data analysis, based on age, benefit elections, etc. Contractors - Direct Contractors perform duties as assigned within the system.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	OCIO Azure GSS uses the Role-Based Access Control (RBAC) procedures to authorize system users' access to PII. These roles limit the user's functionality and access to only that which is required to perform their job. Roles are granted by CDC supervisory personnel.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Monitored by the Network and IT security controls which is administered by CSPO and Infrastructure Services Branch (ISB) who have signed Rules of Behavior and performed the required training, are able to access the system contents for authorized purposes (such as e-discovery or detection of breaches). 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.

PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	System owners, system administrators, managers, contractors and program managers using the application undergo mandatory annual Security and Privacy Awareness Training (SAT), CDC Records Management Training and Role Base Training (RBT) to maintain their CDC network account and access to People Processing.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Users also are required to undergo mandatory annual CDC Records Management Training. In addition, users with significant security responsibilities are required to undergo Role Based Training (RBT).
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	All official records are transferred or destroyed based on CDC record management policies and practices. The following records schedule applies to the system: GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records. This schedule covers records of a transitory or intermediary nature. Transitory records are routine records of short term value (generally less than 180 days). Intermediary records are those involved in creating a subsequent record. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative: Records are maintained according with CDC's record control schedule and record control policy. In addition, the application follows GRS 5.2 020. The PII is secured using the CDC Active Directory authentication process and RBAC. Technical: Monitored by the Network and IT security controls which is administered by CSPO and Infrastructure Services Branch (ISB). Physical: Properties and buildings are protected by guards. Access to grounds and building is controlled by ID badges and key card restrictions.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/20/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/21/2026
SOP Review Comments:	Approved on behalf of Beverly Walker	**# of Days - SOP Review:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/26/2026
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 5/26/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	5

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/29/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/29/2026 3:13 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 06	Data Feed Service, pta_pia_CDC_Release	5/14/2026	Please refrain from using technical jargon since this document is meant for the public. There is information below that can be reworded or removed. Please review and only state the data types and categorize their uses. In addition, the Azure public cloud	

			platform had previously received a Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authorization to Operate (ATO), enabling government agencies and partners to deploy moderately sensitive data to the cloud. Customers can choose either compliant environment to best meet their needs for security and isolation, with assurance that control requirements are being met by comprehensive continuous monitoring and a standardized approach to risk management in both the public and government-community clouds. For additional information, visit the Microsoft Compliance blog and Azure Trust Center, or refer to Azure Federal Risk and Authorization Management Program (FedRAMP) Package ID# F1209051525. The following services are Federal Risk and Authorization Management Program (FedRAMP) authorized and approved by the Joint Authorization Board (JAB): KeyVault, ExpressRoute, WebApps, Azure Site Recovery (ASR), Microsoft Azure Backup (MAB), Notification Hubs, Service Bus, StorSimple, Automation, Azure Resource Manager (ARM), Batch, Media Services, Policy Administration Services (PAS), Scheduler, Log Analytics, and Redis Cache.
PIA 22A	Data Feed Service, pta_pia_CDC_Release	5/14/2026	Please replace Gender with Sex. Ensure this change is also reflected within the rest of the PTA and PIA.
PIA 31A	Data Feed Service, pta_pia_CDC_Release	5/14/2026	The OMB number has expired, please update the expiry date.
PIA 37	Data Feed Service, pta_pia_CDC_Release	5/14/2026	What is the system administrator`s process to determine who has access to the PII? What`s the reason for those individuals to have the access?
PTA 04	Data Feed Service, pta_pia_CDC_Release	5/14/2026	Please describe the function of this system and leave the data list for PTA 5 and 6.
PIA 22	Data Feed Service, pta_pia_CDC_Release	5/14/2026	Add Military Status since it is listed in PTA 4, 5 and 6.

PIA 41	Data Feed Service, pta_pia_CDC_Release	5/20/2026	Are there any technical methods used that you can describe?	
PIA 29B	BLAND, CRYSTAL	5/22/2026	The response didn't sync to OIS, we've emailed CDC Privacy for the response to PIA-29B.	
PIA 29B	BLAND, CRYSTAL	5/26/2026	5/26/2027 Per CDC email, the response is OPM/GOVT-1 General Personnel Records https://www.federalregister.gov/documents/2023/08/17/2023-17651/privacy-act-of-1974-system-of-records	Azure GSS Privacy_Assessment.rtf