Privacy Impact Assessment (PIA): CDC - CDC O365 - QTR1 - 2024 - CDC8017111

Created Date: 7/11/2024 4:01 PM Last Updated: 8/28/2024 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 - CDC O365 - QTR1 - 2024 - CDC8017111	**PIA ID:**	2006409
Name of Component:	CDC - CDC Office 365	**Name of ATO Boundary:**	CDC Office 365
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	174
Submission Status:	Re-Submitted	**Submit Date:**	7/16/2024
Next Assessment Date:	N/A	**Expiration Date:**	8/28/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8017111
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:	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.	CDC has established this cloud computing Software as a Service (SaaS) for the purpose of providing the agency with enhanced email service, electronic collaboration capabilities, and communication tools (hereafter, referred to as CDC Office 365 (CDC O365). In conjunction with the CDC Office 365 (CDC O365) is hosted upon the Microsoft Azure Office 365 Multi-Tenant (O365 MT) FedRAMP approved environment, CDC employs Microsoft Government-only cloud services which align with the descriptions provided by the National Institute of Standards and Technology (NIST) in Special Publication 800-145 (defining cloud computing). CDC's use of the O365MT Software as a Service improves in the agency's continuity of operations, and increases collaboration, efficiency, agility, innovation, and cost savings, for email and office productivity services previously provided by predecessor enterprise email applications and existing collaboration solutions.
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.	Potential types of PII that users may elect to include: Social Security Number, Name, Driver's License Number, Mother's Maiden name, E-Mail Address, phone numbers, medical notes, certificates, education records, military status, foreign activities, taxpayer id, date of birth, photographic identifiers, vehicle identifiers, mailing address, medical records number, financial account info, legal documents, device identifiers, employment status, or passport number. These categories only apply as a user may choose to include such information and unspecified PII in an email message, although it is not required by the information system. Active Directory credential information (UserID) and IP address to allow for mailbox synchronization and email delivery may also be included. Information maintained within CDC O365 includes User identifier, first, middle and last name, organization, office number, email address, IP address, and their individual work phone number. Within the Microsoft Teams component, Equal Employment Office (EEO) legal documents will also be included. These legal documents will include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. These documents may include CDC employee names, mailing address, date of birth, medical records number, financial information related settlement agreements, and employment status. Business contact information on external parties related to the cases, such as professionals (attorneys, doctors, representatives), and witnesses who may include public citizens.

PTA - 5A:	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. The system providing credentials is
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.	CDC O365 stores or passes PII and any other information (text, images, uniform resource locators (URL), attachments, etc.), contained in emails between individual users sending and receiving emails on the system. Individual users control the content of messages they send and must adhere to applicable law and policy, including the Health and Human Services (HHS) Rules of Behavior when using the email service. The nature of the information transmitted will vary widely, as users work in a variety of roles and subject matter areas. Since the information is not required by the system but is incidentally collected as a result of the nature of the application, no definitive purpose can be surmised other than to meet the specific needs of the individual user/sender. User identifier, first, middle and last name, organization, office number, email address, IP address, and users individual work phone number are collected for user identification, authentication, and account maintenance. CDC employee names, mailing address, date of birth, medical records number, financial information related to settlement agreements, employment status, and business contact information for professionals are collected for legal documents related to CDC EEO cases, including complaints, settlements, alternative dispute resolutions, and reasonable accommodations.
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)?	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.	CDC has established this cloud computing Software as a Service (SaaS) for the purpose of providing the agency with enhanced email service, electronic collaboration capabilities, and communication tools (hereafter, referred to as CDC Office 365 (CDC O365). In conjunction with the CDC Office 365 (CDC O365) is hosted upon the Microsoft Azure Office 365 Multi-Tenant (O365 MT) FedRAMP approved environment, CDC employs Microsoft Government-only cloud services which align with the descriptions provided by the National Institute of Standards and Technology (NIST) in Special Publication 800-145 (defining cloud computing). CDC's use of the O365MT Software as a Service improves in the agency's continuity of operations, and increases collaboration, efficiency, agility, innovation, and cost savings, for email and office productivity services previously provided by predecessor enterprise email applications and existing collaboration solutions. All CDC personnel has access to utilize O365 resources.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
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?	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.	Social Security Number Name Mother Maiden Name Email Address Phone numbers Certificates Education Records Military Status Taxpayer ID Date of Birth Photographic Identifiers Vehicle Identifiers Mailing Address Medical Records Number Financial Account Info Legal Documents Employment Status Passport Number User Credentials Driver License Number Other - Free text Field - Medical records (not PHI).
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 Members of the public
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?	The limited PII collected outside of transmitted message content is used primarily for authentication, inbox synchronization and message delivery. For example, Active Directory credential information is used by the system for authentication purposes only. The uses of PII transmitted in the context of messages is as varied as the functions and activities of CDC, from administrative to regulatory to educational and others. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. These documents contain PII, which may include names, mailing address, date of birth, medical records number, financial information related settlement agreements, and employment status. The primary purpose the PII is meet the standard information collected to adjudicate EEO matters and required for other documents in the EEO scope, such as reasonable accommodations and alternative dispute resolutions.
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.	Not Applicable. SSN is not requested or required as part of the agency's or individuals' use of this system. SSNs may be transmitted in individual emails, but not according to any particular, defined use.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable. SSN is not requested or required as part of the agency's or individuals' use of this system. SSNs may be transmitted in individual emails, but not according to any particular, defined use.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. Section 301 which provides authority for the agency to establish the organizations, procedures and tools necessary to perform its duties and pursue its mission. Information use and disclosure for this system is governed by the laws and regulations of the individual business practice that this system is used to conduct. Users work in various agency organizations that have different functions and are subject to different laws and regulations. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. Legal authorities include Executive Order 11478, 42 USC 2000e and 29 USC 633a.
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.	09-90-0009, "Discrimination Complaints Records"
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Email Online Other Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Other Federal Entities Non-Government Sources Members of the Public Private Sector
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.	Not Applicable; due to CDC O365 into itself is not the owner of the PII question where it's not specifically being collected to support a specific event or activity.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies Within HHS

PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Within HHS: Email address and content are shared as part of normal communication. Content of email varies with business function. EEO legal documents including complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases may be shared with HHS EEO staff via the HHS iComplaints system, which is used to track EEO cases Department-wide. Other Federal Agency/Agencies: Email address and content are shared as part of normal communication. Content of email varies with business function. State or Local Agency/Agencies: Email address and content are shared as part of normal communication. Content of email varies with business function. Private Sector: Email address and content are shared as part of normal communication. Content of email varies with business function.
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)).	The agreements governing information exchange will vary with the business functions and purposes of exchanging email. Memorandum of Understanding and Information Sharing Agreements may be used as directed by policy with other HHS OpDivs with whom CDC interacts. For EEO and related cases, the CDC employee is required to complete a Designation of Representation Form in order to authorize information sharing and disclosure of case information to external professionals (attorneys, doctors, representatives).
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.	CDC O365 may be required to make such disclosures in the event that discovery is required pursuant to legal action; if needed to respond to public health or other national emergencies; or to investigate security or privacy incidents/breaches. Such requests can be performed by an approved System Administrator; an accounting of responses for such disclosures will be managed through the existing management processes within CDC Digital Services Office (DSO). For EEO and related cases, the Designation of Representation Forms are stored and accounted for outside of the CDC O365 system.
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.	Voluntary: No PII data is specifically collected or used throughout the use of an email system; 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 business processes underlying the use of an email service. Voluntary: For EEO and related cases, PII collection is required for case processing and adjudication. However, if the individual declines to share PII, he or she may not initiate an EEO complaint.
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.	No major changes to CDC O365 are planned or anticipated. No PII data is specifically collected or used throughout the use of an email system; therefore, there are no CDC O365 specific notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of an email service and is the responsibility of the organization administering the business process. For EEO and related cases, individuals and organizations which consulted an EEO counselor or filed a formal allegation of discrimination are aware of that fact. They may write the appropriate system manager indicated below or the general coordinator if the immediate system manager is unknown, regarding the existence of such records pertaining to them and if major changes have occurred to the system. System Manager: Centers for Disease Control EEO Officer, Room 2405, Building 1, 1600 Clifton Road, NE., Atlanta, Georgia 30333
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.	The process in place for resolving an individual's concerns is to: Contact the CDC Privacy Office at privacy@cdc.gov (or by phone at 770-488-8660) , reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. For EEO and related cases, individuals may also write the appropriate system manager indicated below or the general coordinator if the immediate system manager is unknown: System Manager: Centers for Disease Control EEO Officer, Room 2405, Building 1, 1600 Clifton Road, NE., Atlanta, Georgia 30333

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.	Review of PII transmitted in the email system would not be efficient or appropriate. Data integrity is maintained at the level of the business process, or through maintenance of the applications that support business processes. The Active Directory information used by CDC O365 originates from a separate information system which has its own processes for maintaining integrity, availability, accuracy and relevancy. Agency-wide cybersecurity, physical security, continuing operations and other measures also support data integrity and availability and system functionality. Users are responsible for the accuracy and relevancy of PII they transmit over CDC O365. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. These documents contain PII, which may include names, mailing address, date of birth, medical records number, financial information related settlement agreements, and employment status. The EEO case managers periodically review the EEO legal documents (including PII) for assigned cases on an annual basis, to ensure that only those records that are relevant and necessary are maintained; that all records used to make a determination about an individual are sufficiently accurate, relevant, timely, and complete to make a fair decision; and that all records disclosed outside CDC are consistent with disclosure requirements of SORN 09-90-0009 "Discrimination Complaints Records, HHS/OS/ASPER"
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: To send and receive email and perform duties. Within the Microsoft Teams component: CDC OEEO staff who require access to complaints, settlements, alternative dispute resolution, and reasonable accommodation documents for CDC EEO cases. Administrators: CDC administrators provide Tier 4 Help Desk support which may require performing queries related to PII. Contractors: Offsite (indirect contractors) Microsoft Cloud Service provider support personnel (system administrators) have access to PII in order to provide technical support upon CDC request.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users (i.e., those authorized to send and receive emails) and administrators that have completed CDC onboarding and personnel security processes, including security awareness and privacy training, are able to access the contents of emails that they receive or create. Additionally, Role Based Access Controls 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, such as the various support desk tiers, can perform job functions which might allow access to PII information. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. Access to and use of these records are limited to those persons whose official duties require such access. The EEO Resource Manager determines which OEEO staff require access to specific Teams folders and documents.

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.	This is a standard email system, and emails are sent from user to specified recipients. Other parties (system administrators, contractors, users not party to a specific communication, etc.) will not have access to emails not specifically addressed 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. CDC O365 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. 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. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. Access to and use of these records are limited to those persons whose official duties require such access. The EEO Resource Manager determines which OEEO staff require access to specific Teams folders and documents and grants the minimum level of access accordingly.
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 training regarding the basic concepts of accessing email and collaboration services offered by the CDC O365 cloud-based solution. CDC O365 Administrators are required to complete 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).	Email messages and content that constitute a federal record which CDC is obligated to preserve will be subject to a variety of record retention schedules specific to each business use. Each agency user is responsible for adhering to the schedules that apply to the records under their control. Beyond PII maintained under an approved records schedule, users have the ability to archive messages containing PII on their workstation or in their mailbox indefinitely. Otherwise, the data retention policy on the CDC O365 storage arrays is 14 days. If a user deletes a message, at which time it is moved to the Deleted Items Recovery folder for 14 days. After this period, the deleted mail is stored in a purge folder for 14 days, during which time only authorized administrators can access it. The General Records Schedule (GSR) 5.5, item 10 (DAA-GRS-2016-0012-0001) and item 020 (DAA-GRS-2016-0012-0002) provide the specific retention schedules. GRS 5.5, item 10 Disposition Authority: DAA-GRS2016-00120001. Destroy when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use. GRS 5.5, item 20 Disposition Authority: DDAA-GRS2016-00120002. Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use. Within the Microsoft Teams component: SORN 09-90-0009, "Discrimination Complaints Records, HHS/OS/ASPER", Retention and disposal: The records are retained for four years after final disposition, and are then destroyed. (See HHS Personnel Instruction 293-1, Exhibit X293-1-1, item 26a(1).)

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.	CDC O365 implements security controls to protect PII, as defined by OMB mandates, the Federal Information Security Management Act (FISMA), and NIST Special Publications (SP) 800-53, 800-37, 800-122, NIST Federal Information Processing Standards (FIPS) 200, 201, 199, 197, 140-2, and other associated documents as outlined by Federal Risk and Authorization Management Program (FedRAMP) (www.fedramp.gov). 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, users can encrypt email traffic, including those messages containing PII, in accordance with applicable CDC policies. TECHNICAL CONTROLS: Technical controls applied to CDC O365 include: continuous network/system monitoring; anti-malware; spam and email content filtering; FIPS 140-2 compliant encryption of data in transit; firewalls; Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Data Loss Prevention (DLP); and multi-factor authentication. PHYSICAL CONTROLS: Physical controls include: Hosting within data centers which control and monitor physical access to the system components, including security guards, 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:**	7/18/2024
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:**	8/7/2024
		SOP Days Open:	22

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/12/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 8/12/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	5

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	8/28/2024
		SAOP Days Open:	16

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	7/11/2024	Slightly edited for clarity.	
PIA - 8A	Data Feed Service, piafrmcdc	7/11/2024	Please specify.	
PIA - 10	Data Feed Service, piafrmcdc	7/11/2024	OMB number is required when information is solicited from the public. Please talk to your Paperwork Reduction Act (PRA) Point of Contact for more information.	
PIA - 10C	Data Feed Service, piafrmcdc	7/11/2024	If this system or collection is exempt from the PRA, you must cite the reason for exemption here.	
PIA - 10C	Data Feed Service, piafrmcdc	7/16/2024	Non-responsive.	

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:	8/28/2024 8:01 PM	**History Log:**	View History Log