Attachment 8: FMS Privacy Impact Assessment

Privacy Impact Assessment (PIA): CDC - Azure Dynamics - QTR3 - 2024 - CDC8414656

Created Date: 8/9/2024 9:58 AM Last Updated: 12/27/2024 3:00 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

Does this need to migrate to a Sub-Component?:	No

Consolidated Parent Component

Component Name
No Records Found

General Information

PIA Name:	CDC - Azure Dynamics - QTR3 - 2024 - CDC8414656	**PIA ID:**	8414656
Name of Component:	CDC Azure Government with Dynamics 365	**Name of ATO Boundary:**	CDC Azure Government with Dynamics 365

Migrated Sub-Component PIA

PIA Name
No Records Found

Sub-Component

Software Name
No Records Found

Original Related PIA ID

PIA Name
No Records Found

Overall Status:		**PIA Queue:**	
Submitter:	BROWN, Lashell SIZEMORE, Curtis	**# Days Open:**	140
Submission Status:	Re-Submitted	**Submit Date:**	12/11/2024
Next Assessment Date:	12/27/2027	**Expiration Date:**	12/27/2027
Office:	OD	**OpDiv:**	CDC
Security Categorization:	Moderate		
Legacy PIA ID:		**Make PIA available to Public?:**	Yes
1:	Identify the Enterprise Performance Lifecycle Phase of the system		
2:	Is this a FISMA-Reportable system?		
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		
4:	ATO Date or Planned ATO Date		11/27/2024

Privacy Threshold Analysis (PTA)

PTA Name
CDC - Azure Dynamics - QTR3 - 2024 - CDC8414631

History Log:	View History Log

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 allowing users to coordinate workflow and develop metrics for the sales and marketing efforts within an organization hereafter, referred to as CDC Azure Government with Dynamics 365 (CDC Azure Dynamics). In conjunction with the CDC Azure Dynamics is hosted upon the Microsoft Azure Customer Relationship Management (CRMOL) 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 CRMOL Software as a Service improves 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.	The CDC Azure Dynamics 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 their respective tenant environment. Communication 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). The CDC Azure Dynamics system itself does not include its own Active Directory (AD) server. Rather, it interconnects to the agency's existing Active Directory infrastructure in order to manage and authenticate user access to CDC Azure Dynamics. AD is a separate system and covered by its own PIA.
PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a sep
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 Azure Dynamics is a Major Application (MA) supporting the transfer of messages among users of the system. Staff can send messages to other CDC staff members or externally to other email users; that is to say, this email system will have all the capabilities expected of other email systems. CDC Azure Dynamics stores or passes PII and any other information (text, images, uniform resource locators (URL), attachments, etc.), contained in content shared between individual users sending and receiving information on the system. Individual users control the content of what they send and/or receive and must adhere to applicable law and policy, including the HHS Rules of Behavior when using the service. The nature of the information transmitted will vary widely, as users work in a variety of roles and subject matter areas. Transmitted information is stored on the service provider's cloud servers. Users control whether and for how long they maintain the information in their CDC Azure Dynamics tenant space. The information types identified for the system's FIPS 199 Security Categorization as documented in the Baseline System Information document include: Central Records and Statistics Management Lifecycle/Change Management Information Sharing Access to Care Population Health Management and Consumer Safety Health Care Administration Health Care Research and Practitioner Education Workforce Planning Note that under some analyses, an agency use of an email service would be considered not to involve the collection, maintenance, use, or sharing of PII, but to be the use of a "common carrier" that merely transmits the PII in the service of other business practices and applications
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No

PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	CDC has established this cloud computing Software as a Service (SaaS) for the purpose of allowing users to coordinate workflow and develop metrics for the sales and marketing efforts within an organization hereafter, referred to as CDC Azure Government with Dynamics 365 (CDC Azure Dynamics). In conjunction with the CDC Azure Dynamics is hosted upon the Microsoft Azure Customer Relationship Management (CRMOL) 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 CRMOL Software as a Service improves 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 have access to utilize CDC Azure Dynamics 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.	Session Cookies - Does Not Collect PII
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government website external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	

PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	Yes
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers User Credentials Other - Free text Field - Gender CDC Center or
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.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The CDC Azure Dynamics 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 their respective tenant environment. CDC Azure Dynamics is a Major Application (MA) supporting the transfer of messages among users of the system, which includes PII such as names, email addresses, phone numbers, and user credentials. Staff can send messages to other CDC staff members or externally to other email users; that is to say, this email system will have all the capabilities expected of other email systems. The limited PII collected outside of transmitted message content is used primarily for authentication. For example, Active Directory credential information is used by the system for authentication purposes only.

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 and/or Taxpayer ID.	NA
PIA - 6A:	Cite the legal authority to use the SSN.	NA
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 U.S.C. 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.
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.	The PII data elements listed below are used to retrieve records. -Name, Email addresses, phone number, date of birth, passports, and Gender, CDC Center or Division, type of action, date issued, days suspended, union status, arbitration dates, case status, final decision amount and date, adverse action comment, and WRO user that created the work stream, race, employment type and CDC Id.
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	OPM/GOVT-3: "Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers" Also, SORN 09-90-2301 "Personnel (Employee and Non-Employee) Recruitment Program Records" https://www.federalregister.gov/documents/2023/04/04/2023-06900.
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains 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.	The system does not independently collect or maintain PII from the public. It only facilitates authentication and access control through Active Directory and PII collection occurs at the tenant level, with each tenant responsible for their own OMB approval.
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.	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 authorize 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 Azure Dynamics 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 Azure Dynamics 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 individuals to 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 individual tenant residing upon the CDC Azure Dynamics system is responsible for obtaining consent and/or providing notification that providing PII is voluntary and can opt out from providing the data. Obtaining consent and/or providing notification is part of the business processes underlying the use of the service and is the responsibility of the organization administering the business process.
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 Azure Dynamics are planned or anticipated. No PII data is specifically collected or used throughout the use of the system; therefore, there are no CDC Azure Dynamics 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 the service and is the responsibility of the organization administering the business process.
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 OEEOWE 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 Office of Equal Employment Opportunity and Workplace Equity (OEEOWE) 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.	The Active Directory information used by CDC Azure Dynamics 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, availability and system functionality. Users are responsible for the accuracy and relevancy of PII they transmit over CDC Azure Dynamics.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	Third-Party Contractor (Contractors other than HHS 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. Administrators: CDC administrators provide Tier 4 Help Desk support which may require performing queries related to PII. Contractors: Offsite indirect contractors (non-HHS/CDC credentialed) 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 and administrators that have completed CDC onboarding and personnel security processes, including security awareness and privacy training, are able to access their assigned tenant space. 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.

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.	The Cloud Service providers personnel system administrators, contractors, users not party to a specific communication, in particular are not to have any access to the content of tenant space but are expected to perform support functions to maintain the underlying service into itself. CDC Azure Dynamics system administrators with the appropriate permissions, who have signed Rules of Behavior and performed the required training, are able to access the contents of tenants, for authorized purposes such as stand up of tenant space and/or troubleshooting issues. 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 - 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 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 Azure Dynamics cloud-based solution. CDC Azure Dynamics 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).	Information 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 Azure Dynamics storage arrays is 14 days. If a user deletes an entry, at which time it is moved to the Deleted Items Recovery folder for 14 days. After this period, the deleted entry 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.

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 Azure Dynamics 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); 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:**	12/17/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor)	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	JWO Signature.docx
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	12/18/2024
		SOP Days Open:	7

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	12/20/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 12/20/2024 The comments are for updates on the next iteration of the PTA. The PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:	Approved on behalf of Bridget Guenther	**SAOP Review Date:**	12/27/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 8	MOSIOS, Joshua	8/12/2024	Is this no longer a system of record? The previous PIA cited "09-90-0059, Federal Advisory Committee Membership Files" and "OPM/GOV'T 3 Records of Adverse Actions". If there has been a significant change in how this system manages information, please describe that change in a comment (yellow note pad). I will add that information to PTA 2A, which details changes in the system. If this is	

			still a System of Record, please update this answer.
PIA - 10C	MOSIOS, Joshua	8/12/2024	Please clarify answer. Document this system's exemption from the Paperwork Reduction Act (PRA).
PIA - 11C	MOSIOS, Joshua	8/12/2024	Please cite the actual MOUs and ISAs, as applicable.
PIA - 1	MOSIOS, Joshua	8/12/2024	Delete "user ID' from the free text field and select "user credentials"
PIA - 4	OSHODI, Jarell	9/12/2024	The purpose appears to be broad; however, the PII listed appears to be very specific to certain types of records. Based on the PII listed, what is the purpose of that PII as well?
PIA - 8A	OSHODI, Jarell	9/12/2024	For the purposes of the Privacy Act, which direct identifier is used to retrieve the records? Most of the data elements listed are not direct identifiers.
PIA - 8B	OSHODI, Jarell	9/12/2024	Based on the info provided, I do not see how 09-90-0059, Federal Advisory Committee Membership Files applies. If it does not apply, please delete it.
PIA - 10C	OSHODI, Jarell	9/12/2024	The response is not clear. Are you trying to say that the system does not independently collect or maintain PII from the public? It only facilitates authentication and access control through Active Directory and PII collection occurs at the tenant level, with each tenant responsible for their own OMB approval?
PIA - 16	OSHODI, Jarell	9/12/2024	Is there a reason to keep the first sentence?
PIA - 15	OSHODI, Jarell	9/12/2024	EEO is no longer being used. It is now the Office of Equal Employment Opportunity and Workplace Equity.
PIA - 4	OSHODI, Jarell	9/12/2024	Also, for clarity, specify the category of individuals' PII if there are multiple purposes.
PIA - 1	Data Feed Service, Sync2PIAForm	12/20/2024	On the next iteration of the PTA update the following: PTA-5: Please list the PII elements that are listed in PIA-1 in your response. PTA-5A: Select "Yes, but user credentials are maintained by another

system ...."