PTA / PIA: OS - DMIS - QTR4 - 2025 - OS3137334

Created Date: 11/21/2025 4:03 PM Last Updated: 12/9/2025 4:01 PM

General Information

PTA / PIA Name:	OS - DMIS - QTR4 - 2025 - OS3137334	**PTA / PIA ID:**	4034332
Component Name:	OS - OS - OS - Disaster Medical Information Suite	**ATO Boundary Name:**	Disaster Medical Information Suite
Overall Status:	Complete	**# of Days - Open:**	64
Submitter:		**Submit Date:**	11/21/2025
Next Assessment Date:	12/08/2028	**Expiration Date:**	12/8/2028
Office:		**OpDiv:**	OS
Security Categorization:	Moderate		
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.	10/11/2027
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Helga Scharf-Bell
PTA 01A:	POC Title and Organization	System Owner ORG: ASPR/CFR/ONDMS
PTA 01B:	POC Email Address	Helga.scharf-Bell@HHS.gov
PTA 01C:	POC Phone Number	202-436-6959
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.	2021- National Disaster Medical System (NDMS) 2.0 was released and involved the decoupling of the back-end and the presentation layer of the application infrastructure. This frees the NDMS to grow and expand and use new technologies (both software and hardware), and to share data between applications. The biggest benefit to NDMS users would be a single sign-on. NDMS would stop being nine independent applications and become one NDMS Enterprise application with many applets tailored to the user's needs.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
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.	Disaster Medical Information Suite (DMIS) functions as the Electronic Health Record (EHR) and Patient Movement System for the Office Assistant Secretary for Preparedness and Response (ASPR), Office of Emergency Operations (OEM) & National Disaster Medical System (NDMS) to support Emergency Support Function #8 (ESF-8). DMIS is comprised of three interdependent (non-Child) applications. Electronic Medical Record (EMR), Joint Patient Assessment and Tracking System (JPATS), the Health Information Repository (HIR). The HIR database is the central repository for all data for EMR and JPATS within the DMIS suite, the HIR web application is used to view data after it is transmitted to the HIR database. These function as a single system as none can function without the other as a standalone application. EMR is the clinical provider interface (JAVA thick client) for documenting Patient treatment in the field, JPATS is a web application for initiating and tracking patient movement; and HIR is the single repository for patient heath information (PHI) created within the DMIS suite, it also serves as a clinical dashboard Graphical User Interface (GUI) for post deployment review by NDMS medical Support Branch and Chief Medical Officer (CMO). DMIS primary Purpose is to provides ASPR with the ability to obtain, interpret, and use real time response related medical data to include PHI that is critical to the success of the Health and Human Services (HHS) & ASPR ESF-8 support mission. ESF #8 ; Public Health and Medical Services provides the mechanism for coordinated Federal assistance to supplement State, tribal, and local resources in response to a public health and medical disaster, potential or actual incidents requiring a coordinated Federal response, and/or during a developing potential health and medical emergency. These three non-child systems will have their own PIA's based on the type of PII maintained.
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	The information collected in the DMIS systems is provided directly from the patient or someone

	information is PII and how long that information is stored.	accompanying them when they present at a treatment facility. The types of information the system includes: name, addresses, date of birth, Photo, driver's license number, social security number, prior medical history, history of present illness, current medications, allergies and all treatment information. The treatment information includes, but not limited to, symptoms, vital signs, diagnosis, procedures, orders, and medications prescribed. The medical records could also include x-rays, labs results, and provider's comments relative to their observations about the patient. The data in DMIS contains PHI & PII, as described (not Employees or contractors PII or PHI unless they are patients and treated during Response operations). The number of individuals whose PII is in the system can vary widely. The information is collected and used on an emergency basis and not retained on EMR laptops used in the field, but is retained in HIR until no longer needed for public health response reporting. The maximum number of individuals is not expected to ever exceed update to NDMS Medical Services and Chief Medical Officer (CMO) 100,000. All patients, and anyone accompanying them, are documented in a DMIS system for accountability (caregivers first & last name and phone number, for accompanying patients being transported). This is a required option to make sure HHS has records for who is in their care and to make sure there are adequate resources are provided. This system (DMIS) and its applications do not collect employee or direct contractor information other than first, and last name & government email (HHS) (credentials) to initiate a new user account request, this information is maintained in the system. After each use (national security events, disasters or trainings) the deployed systems (EMR) are re-imaged and returned to baseline image (i.e.., no data from past use is kept in EMR data base, the EMR Servers are returned to 'baseline' configuration with no data), with no user (PII) or Patient (PHI) information maintained on Electronic Medical Record Clients. All Data is maintained in the DMIS health information repository (HIR) Data Base (DB). Electronic Medical Record (EMR), Joint Patient Assessment and Tracking System (JPATS), the Health Information Repository (HIR). The HIR database is the central repository for all data for EMR and JPATS within the DMIS suite, the HIR web application is used to view data after it is transmitted to the HIR database. A unique, alphanumeric identifier is used for each patient record in HIR that is de-identified when used for reporting purposes. Any information disclosed is only upon request with those entities noted within the DMIS SORN; entities may include, Department of Justice , Department of Defense, Veterans Administration, & Congress. This Privacy Impact Assessment (PIA) covers DMIS; HIR is the database that is linked to JPATS and EMR. The three modules are interdependent and cannot work without the other.

		All DMIS data including EMR are stored in the database indefinitely. The data from EMR which is one of the DMIS applications is synced back to HIR and saved in the database.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Email Address Non-HHS User Credentials Password
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.	DMIS is a system that supports the efforts of the National Disaster Medical System (NDMS). NDMS operates pursuant to 42 U.S.C 300hh-11, and it resides in the Department of Health and Human Services under Assistant Secretary for Preparedness. The NDMS functions under a coordinated effort between HHS, the Department Of Home land Security (DHS), the Department of Justice (DOJ) the Department of Defense (DoD), and the Department of Veteran Affairs (VA) and Congress working in collaboration with the states and other appropriate public or private entities. NDMS members are activated by the Secretary of HHS to provide health services, health-related social services, or other appropriate auxiliary services to respond to the needs of victims of a public health emergency or other cause for activation as described in 42 U.S.C. 300hh-11 (a)(3). In the course of responding to disasters, NDMS collects data that identifies patients, such as name, address, contact information, prior medical history, history of present illness, current medications, allergies and all treatment information. The treatment information includes, but not limited to, symptoms, vital signs, diagnosis, procedures, orders, and medications prescribed. The medical records could also include x-rays, labs results, and provider's comments relative to their observations about the patient. The information is contained in DMIS, which is comprised of three components: -- The Electronic Medical Record (EMR) is a application that is used to record patient information. It is deployed to operate only in the local area of the disaster. -- The Health Information Repository (HIR) is a central repository of patient information used to coordinate EMR and Joint Patient Assessment and Tracking System (JPATS). Data from HIR is not disclosed for any other purpose, except de-identified data for the purposes epidemiology reporting. -- The Joint Patient and Assessment Tracking System (JPATS) provides information on the location of patients, as they are transported from disaster sites to treatment centers or transferred from one center to another. It is Web-enabled but does not receive full patient record, only information relevant to the patient transfer (identification information and an indication of the seriousness of the patient's condition). Information collected is pursuant to the

		Privacy of Act (5 U.S.C. 552a). This system (DMIS) does not collect employee or contractor information other than first and last name & email for the JPATS application, the EMR Application users/clinical providers are loaded (not collected) on-site from team rosters, each EMR Kit is self contained (Client Server and Clients) and users only have access to the system locally, after each event the EMR Kit is re-imaged and returned to baseline image, with no user information maintained. A unique, alphanumeric identifier is used for each patient record in HIR that is de-identified when used for reporting purposes.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://ndmssuite.hhs.gov/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	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.	This site is to allow access to all NDMS responders.
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 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	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 Social Security Number Driver's License Number Biographical Information Name Date of Birth User Credentials Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Phone Numbers (Business) Medical Information Medical Records Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	Military status Photographic identifiers
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 Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
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?	The information collected is used to document all of the treatment provided to the patient while they are in the care of an Emergency Support Function (ESF)-8 provider or injured during a response or event. This information is critical for patient safety and needs to be available to all the groups that may treat the patient along their entire continuum of care. All de-identified Personal Health Information (information without the PII using the Office of the National Coordinator for Health Information Technology (ONC) ''Safe harbor') is used for health epidemiology studies and public health studies as noted in purpose and routine use in the Disaster Medical Information Suite (DMIS) System of Record Notice (SORN). Any information is only disclosed upon request with those entities noted within the DMIS SORN; entities may include, Department of Justice (DOJ), Department of Defense (DoD), Veterans Administration (VA), & Congress. Technology, Office of the National Coordinator (ONC) health studies as noted in purpose and routine use in Notice (SORN). Any information is only disclosed upon entities that may include, Department of Justice (DOJ), Department Congress.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	De-identified PHI may be used to conduct research after an emergency event. All data used for health epidemiology studies and public health studies is done so in accordance with the purpose and routine use previously stated above. Any information is only disclosed upon request with those entities noted within the DMIS SORN; entities may include, DOJ, DoD, VA, & Congress. Any information is only disclosed upon request with Department of Justice (DOJ), Department of Defense (DoD), Veteran Affairs (VA), & Congress.
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	The SSN is used to create the Electronic Medical Record (EMR) which is used to document all of the treatment provided to the patient while they are in the care of an Emergency Support Function (ESF)-8 provider or injured during a response or event.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	The Office of the National Coordinator for Health Information Technology (ONC) release the authorization to use the SSN under Public Health Service Act, primarily section 2812 (42 U.S.C. 300hh-11); Title VI of the Civil Rights Act of 1964 (42) the Disaster Medical Information Suite (DMIS) System of Record Notice (SORN). Only System Administrators or approved Medical Personnel have the ability to utilize the SSN for the purposes of the EMR.

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The PII is collected as part of the Public Health Service's mission to provide emergency care in the event of natural disasters and other events. These activities are authorized under the Public Health Service Act, primarily section 2812 (42 U.S.C. 300hh-11); Title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.); and Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. 794); and E.O. 13527 pertaining to medical countermeasures. National Disaster Medical System (NDMS) Statute, 42 U.S.C. 300hh-11; Title VI of the Civil Rights Act of 1964; and Section 504 of the Rehabilitation Act of 1973. Records disposition of this medical system of record is determined under laws governing federal records through the National Archives, 44 U.S.C. 3303a.42 U.S.C. 300hh-11 creates the National Disaster Medical System. The Responder Management System (RMS) is authorized by Paragraph (B) of 300hh-11, which states that the NDMS shall carry out such ongoing activities as may be necessary to prepare for the provision of services described in subparagraph (A) in the event that the Secretary activates the National Disaster Medical System (NDMS) for such purposes.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Email Government Sources Within the OPDIV State/Local/Tribal Other Federal Entities Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No

PIA 31B:	Explain why an OMB information collection approval number is not required.	Not Applicable: DMIS is a system that supported the efforts of the National Disaster Medical System (NDMS). NDMS operates pursuant to 42 U.S.C 300hh-11, and it resides in the HHS Administration for Strategic Preparedness and Response (ASPR). The NDMS functions under a coordinated effort between HHS, the DHS, DoD, and VA working in collaboration with the states and other appropriate public or private entities. NDMS members are activated by the Secretary of HHS to provide health services, health-related social services, or other appropriate auxiliary services to respond to the needs of victims of a public health emergency or other cause for activation as described in 42 U.S.C. 300hh-11 (a)(3). In the course of responding to disasters, NDMS collects data that identifies patients, such as name, address, contact information, prior medical history, history of present illness, current medications, allergies and all treatment information. The treatment information includes, but not limited to, symptoms, vital signs, diagnosis, procedures, orders, and medications prescribed. The medical records could also include x-rays, labs results, and provider's comments relative to their observations about the patient, information and an indication of the seriousness of the patient's condition). Information collected is pursuant to the Privacy of Act (5 U.S.C. 552a). OMB section 3507 of the Paperwork Reduction Act does not apply.
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.	When patients arrive at a treatment site they authorize their approval to be treated directly in the Electronic Medical Record (EMR). If persons/patients do not want to be identified or do have not capability of answering for themselves they are entered or can be entered at their own request as 'John Doe' or 'Jane Doe'. The system is specifically designed to protect and de-identify patients either per their personal request or per their agency's request. These patients who have requested the PII be de-identified in their EHR are given hard copy records upon discharge which contain a unique patient ID for retrieving treatment records.
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.	When and if major changes to the system occur, the SORN will be updated to reflect these changes and published in the Federal Register for review and comment. Individuals are given a copy of the patient treatment record (PTR) so they can also provide it to their own medical providers.
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.	No formal process is in place. These systems are used under emergency conditions, and only transactionally.

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.	Periodic reviews occur against a form of external reference term within EMR. All patient health Information is maintained and system users PII that is not maintained as part of the treatment, are transmitted and ultimately permanently stored in an encrypted location.
PIA 38:	Identify who will have access to the PII in the system.	Users 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?	No
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: Provide medical care, track patients, manage disaster medical operations Administrators: Maintain system functionality, manage accounts, troubleshoot, perform security monitoring Developers: Test functionality, support enhancements (preferably using masked/synthetic data) for the system Contractors : Support operations, development, maintenance, auditing, and technical troubleshooting for the system
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	DMIS features role-based user access controls, System owners approve ordinary access (i.e...,access permitting the routine uses of the data) based on role. System owners have the ability to grant requests for higher-level administrative access, but the system owner will approve this level of access based only on the requester's role within the organization, i.e..., if the requester has a legitimate business need to access patient records.
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.	Role and position are based on user access controls. The system uses role-based security. Roles of users are specifically defined, and the system will grant appropriate levels of access as required by the role or job to be performed.
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.	All users (users, administrators, contractors and developers), receive initial user training and job action training which include privacy awareness. There are also annual courses for all staff on information systems security awareness (ISSA), and annual role-based training including 'Information Security for Managers' and 'Information Security for I.T. Administrators'.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	There is an additional ad-hoc and on-the-job training for providers apart from the training provided to all users.
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).	General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. Records in this system will be retained in accordance with a schedule approved by the National Archives and Records Administration (NARA File No. EOM-14-5,). This applies to information in HIR only, as EMR data is temporally maintained on site until it is transferred to HIR. CATEGORY A: Patient Care Forms or other Medical Records- Files created by NDMS Disaster Medical Assistance teams (DMATs) during response to an event while treating and caring for victims of that event . The Pandemic and All Hazards Preparedness ACT (P.L. 109-417) modified section 2811 of the Public health Service Act to establish HHS' Office of the Assistant Secretary for Preparedness and Response (ASPR). These records are covered under NARA File No. EOM-14-5, and grouped by individual events, and their cutoff is at end of response activity by the DMAT (s) for a particular event. These records are retired to Federal record center two years after cutoff, and destroyed 75 years after cutoff. CATEGORY B: Completed Patient Tracking Record these records are retired to Federal Records Centers 1 year after cutoff, and destroyed 10 years after cutoff. CATEGORY C: Veterinary Care Records- Files created by NDMS task forces during response while caring for animals affected by the event. These records are retired to Federal Records Centers 1 year after cutoff, and destroyed 10 years after cutoff.

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: DMIS utilizes role-based security and the administrators adhere to a least privilege methodology. TECHNICAL: All users are required to use passwords of moderate to strong strength according to security controls of the Federal Information Security Management Act (FISMA) of 2014. In addition, with Joint Patient Assessment Tracking System (JPATS) 2.0, two-factor authentication (2FA) was added as an extra layer of security in addition to the password. PHYSICAL: All servers are maintained in a secure building with authorized access control for authorized users only. Data from the field DMIS EMR client server is transmitted to the DMIS HIR on a defined basis through a purpose built gateway for DMIS HIR. In addition, the DMIS is secured behind the HHS firewall which is located in an approved HHS data hosting facility. For the DMIS systems, when the systems return from the field, all information is removed from the computers and they are restored as containing an empty database.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	11/21/2025
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	11/21/2025
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	12/1/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 12/1/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	10

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	12/9/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	8

SAOP Signature

Date	User	Type	Name	Original Value	New Value
12/9/2025 2:21 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 02A	Data Feed Service, pta_pia_OS_Release	11/19/2025	Please spell/define NDMS on first use.	
PTA 04	Data Feed Service, pta_pia_OS_Release	11/19/2025	Please spell/define JPATS, GUI, PIA's, and PII on first use.	
PTA 07	Data Feed Service, pta_pia_OS_Release	11/19/2025	This response should be updated to a 'yes', and the PIA portion of the questionnaire should be completed.	
PTA 06	Data Feed Service, pta_pia_OS_Release	11/19/2025	Please remove the extra 'PTA - ' on the end of this response.	
PIA 22	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please also select 'e-mail' and 'medical information' for this response.	
PIA 25	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please refer to my supplemental e-mail I provided regarding missing text from the response.	
PIA 26	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please refer to my supplemental e-mail I provided regarding missing text from the response.	
PIA 28	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please refer to my supplemental e-mail I provided regarding missing text from the response.	
PIA 31B	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please refer to my supplemental e-mail I provided regarding missing text from the response.	
PIA 44	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please refer to my supplemental e-mail I provided regarding missing text from the response.	
PIA 45	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please refer to my supplemental e-mail I provided regarding missing text from the response.	
PIA 39	Data Feed Service, pta_pia_OS_Release	11/21/2025	Please remove the first section of this response before the list. (Everything before the word 'Users")	
PTA 01	VILLAFUERTE, NESTOR	11/25/2025	Is the ATO date listed the expiration of the ATO?	
PTA 01	BLAND, CRYSTAL	12/1/2025	It seems the ATO is expired 11/21/2025.	