PTA / PIA: FDA - PNM - QTR2 - 2026 - FDA5269695

Created Date: 5/5/2026 6:11 PM Last Updated: 5/29/2026 10:16 AM

General Information

PTA / PIA Name:	FDA - PNM - QTR2 - 2026 - FDA5269695	**PTA / PIA ID:**	4458349
Component Name:	FDA - OII Prior Notice Manager	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	35
Submitter:		**Submit Date:**	5/6/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
Office:		**OpDiv:**	FDA
Security Categorization:	High		
Make PIA available to Public?:	Yes	**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?	No
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.	1/13/2025
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Sabrina Mosley
PTA 01A:	POC Title and Organization	Information System Owner Office of Inspections and Investigations (OII)
PTA 01B:	POC Email Address	sabrina.mosley@fda.hhs.gov
PTA 01C:	POC Phone Number	240-731-8624
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.	Since the Privacy Impact Assessment (PIA) was last approved, the Food and Drug Administration (FDA) made the following changes to the Prior Notice Manager (PNM) system: Prior Notice Text Analytics (PNTA) was added as a subcomponent of PNM. Prior Notice Text Analytics is an Amazon Web Services (AWS) GovCloud-based artificial intelligence/machine learning (AI/ML) solution that can identify data entities such as names, email addresses, and phone numbers associated with individuals or firms from Portable Document Format (PDF) documents to further enhance Prior Notice targeting and review processes. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks. This new capability expands PNM's analytical functions by applying AI/ML technology to extract and analyze personally identifiable information (PII) and other relevant data from unstructured PDF documents submitted as part of prior notice transmissions. This enhancement supports the Division of Food Defense Targeting (DFDT) in more efficiently identifying potential risks and irregularities in imported food shipments by automating the extraction of key information that previously required manual review.
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.	The Prior Notice Manager (PNM) is a mission-critical system that supports the Food and Drug Administration's (FDA) Office of Inspections and Investigations (OII) Division of Food Defense Targeting (DFDT) in protecting the United States food supply from potential terrorist threats and ensuring regulatory compliance with imported food shipment requirements. The primary purpose of PNM is to verify portions of Prior Notice (PN) imported food shipment transmissions to ensure regulatory compliance and, more importantly, to assess the risk of intentional contamination by biological, chemical, or radiological agents. The system fulfills requirements established under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which mandates that FDA receive advance notice of food shipments entering the United States. PNM carries out its food defense mission through several key functions. The system implements automatic rules to identify and target potentially high-risk food shipments, notifying reviewers of data irregularities that may indicate contamination risks. It processes over 13 million shipments of food, feed, and food/feed additives per year, with DFDT staff manually reviewing approximately 80,000 of these shipments while the remainder are automatically released using risk-based screening

criteria.

The system integrates with multiple FDA systems, federal external applications, and Customs and Border Protection (CBP) systems, ensuring that users can view information from multiple databases while reviewing prior notice transmissions. This integration provides DFDT analysts with comprehensive information needed to make informed targeting decisions. PNM also ensures that manufacturers of imported food meet the requirements to register in the Food Facility Registration Module (FFRM).

By providing DFDT with the time necessary to review and evaluate Prior Notice submissions before food shipments arrive in the United States, PNM enables improved capabilities to deploy resources to conduct inspections and helps intercept contaminated products before they enter the country's food supply chain, thereby supporting the Department of Health and Human Services' (HHS) mission to protect public health and safety.

PNM system users include internal FDA personnel comprising OII regulatory and compliance personnel, specifically DFDT analysts, as well as system administrators and system development personnel. Administrators are responsible for reviewing, processing, and administering the system, files and data, and access control. Developers are responsible for troubleshooting issues with the system, performance, and access. Contractors include Direct Contractors supporting the Information Technology (IT) team for administration, troubleshooting, and development of the system, who can serve as users, administrators, and developers.

PNM is an internal-facing, Single Sign-On (SSO) enabled application. Authorized FDA users access the system through the FDA's Enterprise Active Directory authentication infrastructure using HHS/OpDiv Personal Identity Verification (PIV) Card credentials rather than through a public Uniform Resource Locator (URL) or separate login process. Users authenticate once through the FDA's SSO system using their agency credentials and then gain access to PNM without requiring a separate username and password for the application. User credentials are not stored in the PNM system itself but are managed and controlled by the FDA Enterprise Active Directory system. PNM maintains user information including person IDs as unique identifiers for users granted PNM access and assigned FDA organizational sequence IDs to support access control and user management, but the actual authentication credentials are stored and managed at the enterprise AD level. This SSO architecture provides enhanced security by centralizing authentication, ensuring that only users with valid FDA network credentials can access the system, and enabling

		centralized access management and audit capabilities. The system is accessible via the internal URL https://ora.fda.gov/pnm. FDA users, including both employees and Direct Contractors, with valid network accounts who require access to OII PNM must obtain formal supervisor approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system. Users' supervisors indicate on user account creation forms the minimum access that is required in order for users to complete their jobs, and the scope of access is restricted based on role-based criteria to ensure users can only access the minimum amount of information necessary to perform their job functions. Prior Notice Text Analytics (PNTA) is an Amazon Web Services (AWS) GovCloud-based artificial intelligence/machine learning (AI/ML) solution that can identify data entities such as names, email addresses, and phone numbers associated with individuals or firms from Portable Document Format (PDF) documents to further enhance Prior Notice targeting and review processes. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	PNM collects comprehensive prior notice data including PN confirmation numbers and entry numbers. Prior notice source information identifies whether submissions originated from Automated Commercial System (ACS) Consumption entries, ACS Non-Consumption entries, Prior Notice System Interface (PNSI) entries, or manual entries. The system tracks closure dates when specific PNs are entered, expiry dates when records expire, and submission dates for screening purposes. The system maintains risk assessment data through its Predictive Risk-based Evaluation for Dynamic Import Compliance Tracking (PREDICT) Dynamic Targeting (PDT) functionality. This includes weighted scores representing final overall risk scores for each line, percentiles indicating final overall risk rankings, and analysis type indicators distinguishing between risk analysis and compliance analysis. PDT rule information encompasses rule identifiers (IDs), rule types, rule names and descriptions, and rule states, which can be active, inactive, inactive expired, inactive disabled, pending, or error. The system stores details of files uploaded for targeting purposes. File status indicators track current processing states including S for Submitted, I for In Processing, E for Error, T for Threat Screening System (TSS) Targeting Completed, D for Deleted from PNM User Interface (UI), and P for Purged. Match counts record the number of matches during targeting using data

elements in uploaded files, and error messages capture any issues encountered during upload or processing. The system maintains TSS screening data including hit flags such as O for Ready to be Processed, I for In Process, Y for Hit, and N for No Hit. TSS screening results store detailed information as outlined in the TSS Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA).

PNM collects firm and facility information including Firm Establishment Identifier (FEI) numbers, registration numbers, addresses, and geocoding data. This information is used to identify and verify entities in the food supply chain, assess facility-level risk based on location, history, and characteristics, and support Geographic Information System (GIS) analysis of risk patterns. The system also maintains PNM user information including person IDs as unique identifiers for users granted PNM access and assigned FDA organizational sequence IDs, which supports access control and user management.

The system collects and maintains various types of personally identifiable information (PII) from FDA employees and direct contractors who use the system, as well as from members of the public and private sector entities involved in importing food products. Business contact information includes email addresses, mailing addresses, phone numbers, and names. Identification information includes biometric identifiers such as fingerprints, retina scans, DNA samples, and facial biometric data, as well as passport numbers, photographic identifiers, and vehicle identifiers such as Vehicle Identification Number (VIN) and license plate numbers. Personal characteristics collected include date of birth, sex, physical characteristics such as tattoos and scars, and disability information. Background information includes criminal records, foreign activities, and citizenship information. This PII is used primarily to identify and verify entities involved in the imported food supply chain for the purpose of assessing food defense risks and ensuring regulatory compliance with Prior Notice requirements. Contact information such as names, phone numbers, and email addresses enables DFDT analysts to conduct outreach when prior notices contain incomplete or questionable data, to verify the legitimacy of food shipments, and to gather intelligence that may indicate intentional contamination risks. FDA employee PII is used throughout the system to ensure accountability for all targeting decisions, note entries, rule configurations, and compliance actions.

The records handled in PNM are governed by a variety of records schedules specific to the nature of the records. The retention and destruction periods generally range from 10 to 30 years after an action closes or when a record is no longer needed. Imports program database records are maintained in accordance with National Archives

		and Records Administration (NARA) approved citation N1-088-09-3, which states that records disposition is temporary, with records deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final. Program management files fall under NARA approved citation N1-088-07-2.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	FDA Enterprise Active Directory SSO system FDA Enterprise Oracle Internet Directory
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	All information collected in PNM serves the core mission of protecting the United States food supply from intentional contamination while ensuring regulatory compliance with Prior Notice requirements. Information is maintained to support accountability, enable effective decision-making, and comply with federal recordkeeping requirements. Sharing occurs only with authorized personnel and systems on a need-to-know basis to support coordinated food defense and regulatory enforcement activities. Prior Notice (PN) transmission data is collected to verify regulatory compliance with FDA requirements for imported food shipments and to assess the risk of intentional contamination by biological, chemical, or radiological agents. This information fulfills the Division of Food Defense Targeting (DFDT) mission of protecting the United States food supply from terrorist attacks and other public health emergencies. The data is maintained to create historical records for tracking and trend analysis, to support compliance actions and enforcement activities, and to enable retrospective review of targeting decisions. Firm and facility information, including Firm Establishment Identifier (FEI) numbers, registration numbers, addresses, and geocoding data, is collected to identify and verify entities in the food supply chain, assess facility-level risk based on location, history, and characteristics, and support Geographic Information System (GIS) analysis of risk patterns. This information is maintained to build institutional knowledge about foreign facilities, track facility compliance history, and support targeting based on shipper and manufacturer track records. Risk assessment data through the Predictive Risk-based Evaluation for Dynamic Import Compliance Tracking (PREDICT) Dynamic Targeting (PDT) functionality, including weighted scores, percentiles, and analysis type indicators, is collected to systematically evaluate the risk level of each imported food shipment. This information enables DFDT analysts to prioritize manual reviews of the highest-risk shipments from among the over

13 million annual submissions, ensuring efficient allocation of limited inspection resources. PDT rule information, including rule identifiers (IDs), types, names, descriptions, and states, is maintained to document the criteria used for risk-based screening, support continuous improvement of targeting algorithms, and provide transparency and accountability in targeting decisions.

File upload information, including file status indicators, match counts, and error messages, is collected to track the processing of data files used for targeting purposes and to identify and resolve technical issues that may affect targeting accuracy. This information is maintained to ensure data integrity and system reliability. Threat Screening System (TSS) screening data, including hit flags and detailed screening results, is collected to identify individuals or entities associated with food shipments who may pose security concerns based on information maintained by the Federal Bureau of Investigation (FBI). This information is shared with DFDT to support enhanced scrutiny of potentially high-risk shipments and is maintained according to the retention requirements specified in the TSS Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA).

Personally identifiable information (PII) is collected about three distinct categories of individuals, each serving different purposes within the system's mission. For members of the public and private sector entities involved in importing food products, business contact information including names, email addresses, mailing addresses, and phone numbers is collected to enable communication with importers, shippers, and other stakeholders regarding prior notice submissions that require clarification, additional information, or present potential food defense concerns. This contact information enables DFDT analysts to conduct outreach when prior notices contain incomplete or questionable data, to verify the legitimacy of food shipments, and to gather intelligence that may indicate intentional contamination risks. Identification information including biometric identifiers such as fingerprints, retina scans, DNA samples, and facial biometric data, as well as passport numbers, photographic identifiers, and vehicle identifiers such as Vehicle Identification Number (VIN) and license plate numbers, is collected to verify the identity of individuals associated with imported food shipments and to support TSS screening for potential security threats. Personal characteristics including date of birth, gender, physical characteristics such as tattoos and scars, and disability information, along with background information including criminal records, foreign activities, and citizenship information, are collected to support comprehensive risk assessment and threat screening activities.

For FDA employees and Direct Contractors who

		use the system, PII including person IDs, assigned FDA organizational sequence IDs, names, and contact information is collected and maintained to support access control, user management, and accountability. This information ensures that only authorized personnel can access the system and enables tracking of all user actions within PNM. FDA employee PII is used throughout the system to ensure accountability for all targeting decisions, note entries, rule configurations, and compliance actions, creating an auditable record of who performed each action and when. Information sharing with other systems occurs to support the integrated food defense mission. PNM integrates with multiple FDA systems, federal external applications, and Customs and Border Protection (CBP) systems to ensure that users can view information from multiple databases while reviewing prior notice transmissions. This integration provides DFDT analysts with comprehensive information needed to make informed targeting decisions. DFDT requires access to the results generated by the TSS application to fulfill its core mission of protecting the United States food supply through proactive, risk-based analysis and targeting. The TSS application's function of identifying and verifying individuals associated with food shipments is a critical data source that directly supports DFDT's analytical and operational responsibilities. An Interconnection Security Agreement between FDA and FBI governs this information sharing, which was renewed on July 29, 2024, and is valid for three years. All information collection, maintenance, and sharing activities are conducted in accordance with applicable legal authorities, including the Federal Food, Drug and Cosmetic Act, 21 United States Code (U.S.C.) 301, as amended by the Food Safety Modernization Act, 21 U.S.C. 220, with relevant provisions at 21 U.S.C. 331 and 350-387, and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), 42 U.S.C. 201. These legal authorities provide the foundation for FDA's collection and use of information necessary to protect the public health and ensure the safety of the food supply.
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).	The Prior Notice Manager (PNM) system is accessible via the following internal URL: **https://ora.fda.gov/pnm** Note that "ora" in the URL refers to the legacy Office of Regulatory Affairs designation, which is now the Office of Inspections and Investigations (OII).

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.	The PNM website is an internal-facing FDA application that supports the Division of Food Defense Targeting (DFDT) in the verification of portions of Prior Notice (PN) imported food shipment transmissions. The primary purpose of the website is to ensure regulatory compliance with Prior Notice requirements and, more importantly, to assess the risk of intentional contamination by biological, chemical, or radiological agents in imported food shipments. The application enables DFDT analysts to review prior notice data, apply risk-based targeting rules including Predictive Risk-based Evaluation for Dynamic Import Compliance Tracking (PREDICT) Dynamic Targeting (PDT) matrix scoring and standard/text targeting, document their findings through various note types, manage compliance actions, conduct Geographic Information System (GIS) analysis of facility locations, and coordinate with other FDA offices and external agencies regarding food defense concerns. The system maintains comprehensive records of all targeting decisions, communications, and compliance actions to support the DFDT mission of protecting the public from threatened or actual terrorist attacks on the United States food supply and preventing food that may be intentionally contaminated from entering the country. Access to the PNM website is restricted to authorized FDA personnel only. Users with access include internal FDA personnel comprising Office of Inspections and Investigations (OII) regulatory and compliance personnel, specifically DFDT analysts, as well as system administrators and system development personnel. Administrators are responsible for reviewing, processing, and administering the system, files and data, and access control. Developers are responsible for troubleshooting issues with the system, performance, and access. Contractors include direct contractors supporting the Information Technology (IT) team for administration, troubleshooting, and development of the system, who can serve as users, administrators, and developers. The website is not accessible to the public. PNM is a Single Sign-On (SSO) enabled application, meaning that authorized FDA users access the system through the FDA's enterprise authentication infrastructure rather than through a public Uniform Resource Locator (URL) or separate login process. Users authenticate once through the FDA's SSO system using their HHS/OpDiv Personal Identity Verification (PIV) Card credentials and then gain access to PNM without requiring a separate username and password for the application. User credentials are not stored in the PNM system itself but are managed and controlled by the FDA Enterprise Active Directory and the FDA Enterprise Oracle Internet Directory (OID). This

		SSO architecture provides enhanced security by centralizing authentication, ensuring that only users with valid FDA network credentials can access the system, and enabling centralized access management and audit capabilities. The system is accessible via the internal URL https://ora.fda.gov/pnm. FDA users, including both employees and direct contractors, with valid network accounts who require access to OII PNM must obtain formal supervisor approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system. Users' supervisors indicate on user account creation forms the minimum access that is required in order for users to complete their jobs, and the scope of access is restricted based on role-based criteria to ensure users can only access the minimum amount of information necessary to perform their job functions.
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?	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 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?	Yes
PTA 21A:	What are the AI tools and how are they used?	A subcomponent of PNM, PNTA, is an AWS GovCloud-based artificial intelligence/machine learning (AI/ML) solution that can identify data entities such as names, email addresses, and phone numbers associated with individuals or firms from Portable Document Format (PDF) documents to further enhance Prior Notice targeting and review processes. This capability expands PNM's analytical functions by applying AI/ML technology to extract and analyze personally identifiable information (PII) and other relevant data from unstructured PDF documents submitted as part of prior notice transmissions, supporting the Division of Food Defense Targeting (DFDT) in more efficiently identifying potential risks and irregularities in imported food shipments. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

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 Passport Number Vehicle Identifiers (e.g., VIN, license plate number) Biographical Information Name Date of Birth Criminal Records Foreign Activities Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Biometrics/Distinguishing Features Biometric Identifiers (e.g., fingerprints, retina scans, DNA samples) Photographic Identifiers Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Sex Citizenship Physical Characteristics (tattoos, scars) Disability Information Facial Biometric Data Person IDs / FDA Org Sequence IDs
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999

PIA 25:	For what primary purpose is the PII used?	The PII in PNM is primarily used to identify and verify entities involved in the imported food supply chain for the purpose of assessing food defense risks and ensuring regulatory compliance with Prior Notice requirements. Specifically, PII such as contact names, phone numbers, email addresses, and firm representative information is collected and used to communicate with importers, shippers, and other stakeholders regarding prior notice submissions that require clarification, additional information, or present potential food defense concerns. This information enables Division of Food Defense Targeting (DFDT) analysts to conduct outreach when prior notices contain incomplete or questionable data, to verify the legitimacy of food shipments, and to gather intelligence that may indicate intentional contamination risks. Furthermore, PII in the form of FDA employee information is used throughout the system to ensure accountability for all targeting decisions, note entries, rule configurations, and compliance actions.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The FDA makes no secondary use of the PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The Federal Food, Drug and Cosmetic Act, 21 U.S.C. 301, as amended by the Food Safety Modernization Act, 21 U.S.C. 220. Relevant provisions can be found at 21 U.S.C. 331 and 350-387. Also, the agency collects and shares information pursuant to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), 42 U.S.C. 201.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	The PII data elements that are used to retrieve records in the PNM system include names, email addresses, and phone numbers associated with firms, entities, or individuals, which could be members of the public. These data elements come from FBI data that is being used for TSS screening purposes to identify individuals or entities associated with food shipments who may pose security concerns based on information maintained by the FBI.
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-10-0002, Regulated Industry Employee Enforcement 09-90-0777, Facility and Resource Access Control Records

PIA 30:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	Information collected under OMB approval is not submitted directly to PNM. However, Prior Notice Submissions employ FDA Form 3540 under OMB approval No. 0910-0520, expiring 09/30/2026.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	DFDT requires access to the results generated by the TSS application to fulfill its core mission of protecting the United States food supply through proactive, risk-based analysis and targeting. The TSS application's function of identifying and verifying individuals associated with food shipments is a critical data source that directly supports DFDT's analytical and operational responsibilities. This information sharing is governed by an Interconnection Security Agreement between FDA and FBI that was renewed on July 29, 2024, and is valid for three years.
PIA 32C:	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)).	An Interconnection Security Agreement between FDA and FBI is currently in place. It was renewed on 7/29/2024 and is good for three years.
PIA 32D:	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.	The system employs standard audit trail columns across most tables to track data operations: CREATED_BY and CREATE_DATE capture who created a record and when, while MODIFIED_BY and MODIFY_DATE track the most recent modifier and modification timestamp. This provides basic user accountability by linking every create and update operation to a specific user ID (PRSNID), enabling identification of who handled PII-containing records and when. Some tables offer enhanced tracking through history tables (like PNMFIRMSGEOCODEHISTORY) that maintain complete version histories, and additional fields like COMPLETEDATE, APPROVEDBY, ACCESSLEVEL, and LOCKIND that track workflow states, approvals, sensitivity levels, and editing locks.
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.	Individuals provide their contact information as a practical requirement to communicate with FDA and, where appropriate, to have system access. There are no opt-out procedures specific to the Imports systems, including PNM. While FDA requires that regulated entities supply the PII of a point of contact, that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity. The collection of PII in PNM is considered voluntary under the Privacy Act, but it is functionally necessary for individuals and entities that choose to import FDA-regulated food products into the United States. The submission of prior notice information, which includes PII, is required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 for anyone seeking to import food products. Individuals and organizations that do not wish to provide this information have the option of not importing FDA-regulated products. The regulated entities have flexibility in designating which authorized representative's PII they provide as their point of contact, giving them some control over whose personal information is submitted to FDA. This approach balances the regulatory requirement for contact information with individual privacy considerations by allowing organizations to designate appropriate personnel for FDA communications rather than requiring specific individuals' information.
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.	No such changes are anticipated. If the FDA changes its practices about the collection or handling of PII related to the Imports system, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include email to individuals, adding or updating online notices or forms, revising this PIA or other available means to inform the individual.
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.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have several avenues available to resolve the situation including FDA's Employee Resource and Information Center (ERIC) and Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) (FDA personnel only). Individuals may also contact the FDA Privacy Office via email, phone, and standard mail avenues (all listed on fda.gov).

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	Users' PII is required. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Design of forms and webpages to collect/solicit only necessary PII ensure data relevancy. Integrity and availability are protected by security and privacy controls selected and implemented while providing the system with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. OII performs annual reviews to evaluate user access.
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?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: FDA Users have access to review, process, and manage data submissions. Administrators: Review, processing, and administering the system, files and data, and access control. Developers: Troubleshooting issues with the system, performance, and access. Contractors: Supporting the IT team for administration, troubleshooting, and development of the system. This includes both Direct Contractors, as well as FDA employees. Direct Contractors can be users, administrators, and developers regarding the PNM system.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users (employees and Direct Contractors) with valid network accounts who require access to OII PNM must obtain formal supervisor approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.

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.	FDA users' supervisors indicate on user account creation forms the minimum access that is required in order for users to complete their jobs. The scope of access is restricted based on role-based criteria. This means that access permissions are tailored to specific job functions and responsibilities, ensuring that users can only view and interact with the data elements necessary for their particular role within the system. Before access is granted, FDA users (including both employees and Direct Contractors) with valid network accounts who require access to OII PNM must obtain formal supervisor approval and signature. During this approval process, supervisors specifically designate the minimum level of access needed for each user to perform their duties, implementing the principle of least privilege. PNM is a Single Sign-On enabled application where authorized FDA users access the system through the FDA's Enterprise Active Directory authentication infrastructure using Health and Human Services/Operating Division (HHS/OpDiv) Personal Identity Verification (PIV) Card credentials. User credentials are not stored in the PNM system itself but are managed and controlled by the FDA Enterprise Active Directory and the FDA Enterprise Oracle Internet Directory (OID). This centralized authentication architecture provides enhanced security and enables centralized access management capabilities. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system. This regular review process ensures that access privileges remain appropriate to current job responsibilities and that former employees or those who no longer require access have their permissions revoked promptly.

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 system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity, and availability, as well as the handling of data, including any special restrictions on data use and/or disclosure. The FDA Office of Information Management and Technology (OIMT) verifies that individuals successfully complete the training. All FDA personnel, including system owners, managers, operators, contractors, and program managers, complete this mandatory security and privacy awareness training at a minimum of once a year. The Office of Digital Transformation (ODT) tracks completion of the annual course to ensure compliance across the organization. This standardized training ensures that all personnel with access to PII in the PNM system understand their fundamental responsibilities for protecting the sensitive information being collected and maintained.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Informal training on functionality and system use is provided to the users at the district and field office level. This training focuses on how to properly operate the PNM system and utilize its specific features and capabilities for reviewing prior notice submissions, applying targeting rules, and documenting findings. All users are provided guidance on adhering to the Health and Human Services (HHS) Rules of Behavior. This ensures that users understand the specific behavioral expectations and requirements for accessing and using FDA systems, including appropriate handling of sensitive information and compliance with agency policies. Users may obtain additional instruction and guidance from FDA's privacy officials and the agency's privacy program. This provides an ongoing resource for users who need clarification on privacy-related matters, guidance on handling specific situations involving PII, or answers to questions that arise during their work with the system. This supplemental training ensures that users not only understand general security and privacy principles from their annual mandatory training but also know how to apply those principles specifically within the PNM system context and their particular job responsibilities.

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).	The records handled in PNM are governed by a variety of records schedules specific to the nature of the records. The retention and destruction periods generally range from 10 to 30 years after an action closes or when a record is no longer needed. Imports program database records are maintained in accordance with National Archives and Records Administration (NARA) approved citation N1-088-09-3 which states that records disposition is temporary, with records deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final. Program management files fall under NARA approved citation N1-088-07-2.
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 safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of firewalls and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the NIST's Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/6/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/6/2026
SOP Review Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/7/2026
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 5/7/2026 All comments have been addressed. This PIA is ready for SAOP review and approval. 5/6/2026 Please see comments and update accordingly: PTA-5 and PIA-22A: Please replace "Gender" with "Sex" per E.O. 14168	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/29/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	22

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/29/2026 9:10 AM	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 01	BLAND, CRYSTAL	5/6/2026	5/6/2026 FDA's Email and PIA Attached.	5-6-2026 EMAIL_FW_ PTA _ PIA 5269695 is ready for APA Review.pdf OII Prior Notice Manager SOP approved.pdf
PTA 05	BLAND, CRYSTAL	5/6/2026	Please replace "Gender" with "Sex" per E.O. 14168	
PIA 22A	BLAND, CRYSTAL	5/6/2026	Please replace "Gender" with "Sex" per E.O. 14168	