PTA / PIA: FDA - ITACS - QTR2 - 2026 - FDA5271569

Created Date: 6/24/2026 10:12 AM Last Updated: 7/2/2026 6:00 PM

General Information

PTA / PIA Name:	FDA - ITACS - QTR2 - 2026 - FDA5271569	**PTA / PIA ID:**	4592186
Component Name:	FDA - OII International Trade Auxiliary Communication System	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	10
Submitter:		**Submit Date:**	6/24/2026
Next Assessment Date:	07/01/2029	**Expiration Date:**	7/1/2029
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
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.	3/4/2025
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.	The Food and Drug Administration (FDA) has made no changes to Import Trade Auxiliary Communications System (ITACS) since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) was approved.
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 Import Trade Auxiliary Communications System (ITACS) is an external-facing, publicly accessible component of the OII Case and Workload Management (OCWM) system, operated by the Food and Drug Administration (FDA), which is part of the Department of Health and Human Services (HHS). ITACS supports HHS's regulatory mission by serving as a communication and document exchange platform between the FDA and the Import Trade Community. The system provides three primary functions: allowing users to check on the status of an import product entry, submit entry documentation electronically, and submit goods availability information for targeted shipments electronically. By enabling these functions digitally, ITACS provides more specific information about import shipments during the admissibility process, reduces confusion between the Import Trade Community and the FDA regarding the date and location of shipment availability, and eliminates the need to copy, mail, or fax entry documentation to the FDA. This in turn reduces the volume of phone calls inquiring about entry statuses and allows FDA Import Field Staff to focus more on entry review and compliance decision-making. ITACS also includes a sub-component called the Authorization, Roles, and Responsibilities Management Services (ARRMS), which performs authentication and manages roles and responsibilities for firm users who have logged into ITACS through the FDA Unified Registration and Listing System (FURLS) Online Account Administration (OAA) system. Regarding user access, ITACS supports two methods of entry. First, members of the general public can access the system without a registered account by providing a valid FDA OCWM product entry number and completing a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) challenge, which was implemented as a protection against denial-of-service attacks. This method allows users to view or provide information for an import product entry, or upload documents associated with the product. Second, firms and trade community members may register for a username and password through the FURLS OAA portal, which provides more detailed access to import product entry statuses. Registered users authenticate via Multi-Factor Authentication (MFA) using a username, password, and a One-Time Password (OTP). There are currently approximately 600 OAA user accounts that may access ITACS. The system is accessible via its public production Uniform Resource Locator (URL) at https://itacs.fda.gov/itacs.

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.	ITACS collects and maintains a variety of information to support communication and document exchange between the FDA and external stakeholders. This information spans both personally identifiable information (PII) and non-PII categories and encompasses several functional data types necessary for the system's regulatory and operational purposes. User account information, which constitutes the PII component of the system, includes business email addresses and business phone numbers. This information is used primarily to authenticate users, facilitate communication, associate users with regulated firms, send notifications, and maintain audit logs for compliance and accountability purposes. It is worth noting that the system does not collect sensitive PII as defined by HHS, does not collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs), and the FDA makes no secondary use of the PII collected. Beyond PII, ITACS also collects and maintains non-PII data, including firm and Firm Establishment Identifier (FEI) data, entry and submission data, document uploads, communication and notification data, workflow tracking information, audit logs, and integration data shared with connected systems including Entry Review (ER), Entry Review Web Service (ERWS), Document and Records Management System (DRMS), and U.S. Customs and Border Protection (CBP). Records handled within the ITACS system are governed by National Archives and Records Administration (NARA)-approved records schedules. Specifically, imports program database records are maintained in accordance with NARA-approved citation N1-088-09-3, which designates records as temporary and requires that they be 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 N1-88-07-2, with retention and destruction periods that generally range from 10 to 30 years after an action closes or when a record is no longer needed.
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.	FURLS

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.	Information is collected, maintained, and shared within ITACS to support secure communication, document submission, and regulatory processing in furtherance of the FDA's import admissibility mission. The following describes the purpose of each type of information collected and the categories of individuals to whom it pertains. User Account Information (PII): Business email addresses and business phone numbers are collected about three categories of individuals — HHS employees and Direct Contractors, members of the public, and vendors, suppliers, and Third-Party Contractors. This information is collected to support user authentication and access control, facilitate communication between the FDA and system users, associate users with their respective regulated firms, deliver system notifications, and maintain audit logs for compliance and accountability purposes. Firm and FEI Data: This non-PII data is collected to ensure the correct association of users and submissions with the appropriate regulated entities. It supports the FDA's ability to accurately track, and process import entries at the firm level. Entry and Submission Data: This information is collected to track all interactions between the Import Trade Community and the FDA, supporting the review and processing of import product entries throughout the admissibility process. Document Data: Document uploads are collected and maintained to support FDA review of import entry documentation, eliminating the need for physical or faxed submissions and enabling a fully electronic review process. Communication and Notification Data: This information is collected and maintained to enable the system to deliver timely notifications to users regarding the status of their import entries and any required actions. Audit Log Data: Audit data is collected and maintained to ensure accountability and regulatory compliance, providing a traceable record of all system interactions and access events. Integration Data: Information shared with connected systems — including ER, ERWS, DRMS, and CBP — is exchanged to support the broader import admissibility workflow, ensuring that entry status information and documentation are accurately reflected across all relevant regulatory systems.
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://itacs.fda.gov/itacs

PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
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.	ITACS is an external-facing system designed to facilitate electronic communication and document exchange between the FDA and the Import Trade Community. The website serves three primary functions: enabling users to check the status of an import product entry, submit entry documentation electronically, and submit goods availability information for targeted shipments electronically. By providing these capabilities through a web-based interface, ITACS reduces the need for phone calls, eliminates the need to copy, mail, or fax entry documentation to the FDA, and allows FDA Import Field Staff to focus more on entry review and compliance decision-making. ITACS is accessible to the general public, as well as to registered firms and trade community members who have obtained user accounts through the FURLS OAA portal. There are currently approximately 600 registered OAA user accounts that may access ITACS. Additionally, FDA employees, Direct Contractors, administrators, and developers have access to the system for the purposes of reviewing, processing, administering, and maintaining the system and its data. ITACS can be accessed through two methods. First, members of the general public may access the system via the public production URL at https://itacs.fda.gov/itacs by providing a valid FDA OCWM product entry number and successfully completing a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) challenge. This method allows users to view or provide information for an import product entry or upload documents associated with the product, without the need for a registered account. Second, firms and trade community members who require more detailed access may register for a username and password through the FURLS OAA portal. These registered users authenticate via Multi-Factor Authentication (MFA) using a username, password, and a One-Time Password (OTP) to gain access to more detailed import product entry statuses and additional system functionality.
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?	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.	Contact Information Email Address (Business) Phone Numbers (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Members of the public 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 PII collected and maintained within ITACS is used for the following primary purposes: Authentication: PII is used to verify and authenticate users accessing the system, ensuring that only authorized individuals are granted access. Communication: PII is used to facilitate communication between the FDA and system users, including the delivery of system notifications and updates regarding import entry statuses. Firm Association: PII is used to associate users with their respective regulated firms, ensuring that submissions and interactions are correctly linked to the appropriate regulated entities. Notifications: PII is used to send relevant notifications to users regarding the status of their import entries and any required actions. Audit Logs and Compliance: PII is used to maintain audit logs for compliance and accountability purposes, providing a traceable record of all system interactions and access events.
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 following legal authorities govern the use and disclosure of information specific to the ITACS system and program: The Federal Food, Drug and Cosmetic Act (FD&C Act), 21 U.S.C. 301, as amended by the Food Safety Modernization Act (FSMA), 21 U.S.C. 220. Relevant provisions can be found at 21 U.S.C. 331 and 350-387. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), 42 U.S.C. 201, pursuant to which the agency collects and shares information. These legal authorities collectively provide the FDA with the mandate to collect, use, and disclose information in support of its import admissibility and regulatory enforcement mission, including the electronic submission of import entry documentation and the monitoring of import product entries into the United States.
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.	Government Sources Within the OPDIV Non-Government Sources 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.	An OMB information collection approval number is not required for ITACS because the system does not collect PII through a standardized federal form or structured information collection directed at the general public. The PII collected by the system — consisting of business email addresses and business phone numbers — is voluntarily provided by individuals as a necessary condition of registering for and accessing the system through the FURLS OAA portal. This registration process does not constitute a collection of information subject to the Paperwork Reduction Act (PRA) clearance requirements.
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.	Individuals whose PII is collected by ITACS are notified and provide consent through the practical requirement of accessing the system. Specifically, individuals voluntarily provide their PII — consisting of their business email address and business phone number — as a necessary condition of obtaining access to the system and its functionality. It is important to note that participation is entirely voluntary. However, choosing not to provide this information will result in being unable to perform the duties of the job position that requires access to ITACS. In this way, the act of voluntarily registering for and accessing the system serves as the mechanism through which individuals are notified of and provide consent to the collection of their PII. Additionally, ITACS has a posted privacy notice on its website, which further informs users of the agency's privacy practices. Should the FDA make any changes to its practices regarding the collection or handling of PII related to the ITACS system, the agency has committed to adopting measures to provide any required notice and obtain consent from individuals. This may include email notifications to individuals, adding or updating online notices or forms, revising the PIA, or utilizing other available means to inform individuals of any changes to the collection and/or use of their PII.
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 major changes to the ITACS system that would affect the collection or handling of PII are currently anticipated. However, should such changes occur, the FDA has established the following process for notifying individuals and obtaining their consent. In the event that the FDA changes its practices with regard to the collection or handling of PII related to the ITACS system, the agency will adopt measures to provide any required notice and obtain consent from affected individuals regarding the collection and/or use of their PII. The methods through which this notice and consent may be obtained include, but are not limited to: Email notifications sent directly to affected individuals. Adding or updating online notices or forms within the system or on the associated website. Revising the PIA to reflect any changes to the system's privacy practices. Other available means deemed appropriate to inform individuals of changes to the collection and/or use of their PII.

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.	The FDA has established several avenues through which individuals who suspect their PII has been inappropriately obtained, used, or disclosed in ITACS — or who believe their PII is inaccurate — may seek resolution. These avenues are as follows: FDA's Employee Resource and Information Center (ERIC): Individuals may contact ERIC to raise concerns regarding the inappropriate handling of their PII and seek guidance on resolution. Cybersecurity and Infrastructure Operations Coordination Center (CIOCC): Individuals may also contact the CIOCC, which serves as another resource for addressing concerns related to the inappropriate obtaining, use, or disclosure of PII within FDA systems. FDA Privacy Office: Individuals may contact the FDA Privacy Office directly through multiple communication channels, including email, phone, and standard mail, all of which are listed on fda.gov. The FDA Privacy Office serves as a dedicated resource for addressing privacy-related concerns and ensuring that individuals' PII is handled in accordance with applicable laws, policies, and regulations. Together, these avenues provide individuals with multiple accessible options for raising and resolving concerns related to the handling of their PII within the ITACS system, ensuring accountability and compliance with applicable federal privacy requirements.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The FDA has established processes to ensure the integrity, availability, accuracy, and relevancy of PII contained within ITACS. Each element is addressed as follows: Integrity: The integrity of PII within ITACS is protected through the security and privacy controls selected and implemented as part of the system's Authorization to Operate (ATO) process. These controls are selected based on National Institute of Standards and Technology (NIST) guidance and are appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. Additionally, technical safeguards including Multi-Factor Authentication (MFA), firewalls, and network monitoring and intrusion detection tools are in place to protect the integrity of PII maintained in the system. Availability: Similar to integrity, the availability of PII within ITACS is protected through the security and privacy controls implemented as part of the ATO process, in accordance with NIST guidance and FIPS 199. Physical controls also contribute to availability, as all system servers are located at facilities protected by security guards, locked facility doors, and climate controls. Accuracy: Accuracy of PII is ensured through a dual approach. First, individuals are responsible for providing accurate information at the time of registration and are able to correct or update their own PII as needed. Second, the Office of Inspections and Investigations (OII) performs quarterly reviews to evaluate user access and revise access or delete accounts as appropriate, ensuring that the PII maintained in the system remains current and accurate. Relevancy: The relevancy of PII maintained in ITACS is ensured through the application of the Need to Know and Minimum Necessary principles when awarding access to the system. Access is granted and restricted at the individual level based on role-based access criteria, ensuring that only PII that is necessary and relevant to an individual's duties is collected and maintained. The quarterly reviews conducted by OII further support relevancy by identifying and removing accounts and associated PII that are no longer needed.
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 and firms require access to PII in order to review, process, and manage data submissions within the system. This access is necessary to carry out their regulatory and operational responsibilities related to import entry review and compliance decision-making. Administrators: Administrators require access to PII for the purposes of reviewing, processing, and administering the system, its files and data, and access control functions. This access is necessary to ensure the proper management and operation of the system and to maintain appropriate user access controls. Developers: Developers require access to PII for the purposes of troubleshooting issues with the system, its performance, and access. This access is necessary to identify and resolve technical issues that may affect the functionality and security of the system and the PII it maintains. Contractors: HHS/Operating Division (OPDiv) Direct Contractors require access to PII for the purposes of 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 serve as users, administrators, and developers regarding the ITACS system, and therefore require access to PII commensurate with the role they are fulfilling in support of the system's operation and maintenance.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users, including employees and Direct Contractors, who possess valid network accounts and require access to ITACS must obtain formal supervisor approval and signature before access is granted. This ensures that access to PII is authorized at the supervisory level and is granted only to individuals with a demonstrated need to access the system in furtherance of their official duties. The agency conducts quarterly reviews of the system access list to adjust users' access roles and permissions and delete unneeded accounts from the system. These periodic reviews ensure that access to PII remains appropriate and current, and that accounts belonging to individuals who no longer require access are promptly removed. Access to PII within ITACS is granted and restricted based on role-based criteria. A user's supervising official indicates on the user account creation form the minimum level of access required for the user to complete their job responsibilities, ensuring that the Need to Know and Minimum Necessary principles are applied when determining the scope of each user's access to PII. Contracts with HHS/OPDiv Direct Contractors include FAR and other appropriate clauses ensuring adherence to privacy provisions and practices, providing an additional layer of administrative oversight governing contractor access to PII within 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.	The primary technical method in place to limit access to the minimum necessary PII is role-based access control. A user's supervising official indicates on the user account creation form the minimum level of access required for the user to complete their job responsibilities. The scope of access is then technically restricted based on these role-based criteria, ensuring that each user can only access the PII and system functionality that is necessary and relevant to their specific duties. Access to ITACS is protected by MFA, requiring users to authenticate via a username, password, and OTP before being granted access to the system and its PII. This technical control ensures that only authorized individuals are able to access the system and the PII it maintains. Technical safeguards including firewalls and network monitoring and intrusion detection tools are in place to protect against unauthorized access to PII within the system. These controls help ensure that access to PII is limited to only those individuals who have been properly authenticated and authorized to access the system. User credentials and access management for ITACS are handled through the FURLS OAA system, which provides a centralized and controlled mechanism for managing user accounts, roles, and permissions. This technical control ensures that access to PII is granted and restricted in a consistent and auditable manner, in accordance with the role-based criteria established during the account creation process.
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 the FDA are required to complete annual mandatory computer security and privacy awareness training. This training is comprehensive in scope and includes guidance on the following: Federal Laws, Policies, and Regulations: The training covers applicable federal laws, policies, and regulations relating to privacy and data confidentiality, integrity, and availability. Data Handling: The training includes guidance on the proper handling of data, including any special restrictions on data use and/or disclosure that are applicable to the information maintained within ITACS and other FDA systems. The Office of Digital Transformation (ODT) is responsible for verifying that all individuals successfully complete the required annual mandatory computer security and privacy awareness training. This verification process ensures that all personnel with access to ITACS and its PII are aware of and accountable for their responsibilities in protecting the information being collected and maintained by the system.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	The following training above and beyond the general annual mandatory computer security and privacy awareness training: Informal Functional Training: Informal training on the functionality and use of the ITACS system is provided to users at the district and field office level. This training is designed to ensure that users are familiar with the specific features and capabilities of the system and are able to effectively carry out their import entry review and compliance decision-making responsibilities using the system. HHS Rules of Behavior Guidance: All users are provided guidance on adhering to the Health and Human Services (HHS) Rules of Behavior, which establish the standards of conduct and responsibilities expected of all individuals who access HHS information systems and the PII they maintain. FDA Privacy Program: Users may obtain additional instruction and guidance via FDA's privacy program, which serves as a supplementary resource for individuals seeking further information on their responsibilities for protecting PII and other sensitive information maintained within ITACS and other FDA systems. Together, these additional training resources complement the general annual mandatory computer security and privacy awareness training to ensure that all system users are comprehensively informed of their responsibilities for protecting the information collected and maintained within ITACS, both from a technical and regulatory standpoint.

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 within ITACS are governed by a variety of records schedules specific to the nature of the records. Retention and destruction periods generally range from 10 to 30 years after an action closes or when a record is no longer needed. The specific National Archives and Records Administration (NARA)-approved records retention schedules applicable to ITACS are as follows: NARA-Approved Citation N1-088-09-3: Imports program database records, which include PII such as business email addresses and business phone numbers, are maintained in accordance with NARA-approved citation N1-088-09-3. This citation designates records as temporary in nature, with records to be deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final. NARA-Approved Citation N1-88-07-2: Program management files maintained within ITACS are governed by NARA-approved citation N1-88-07-2. Records falling under this citation are subject to retention and destruction periods that generally range from 10 to 30 years after an action closes or when a record is no longer needed. Quarterly Access Reviews: It is worth noting that in addition to the formal NARA-approved records retention schedules described above, OII conducts quarterly reviews to evaluate user access and delete accounts that are no longer needed. This process ensures that PII associated with inactive or unnecessary user accounts is promptly identified and removed from the system in a timely manner, further supporting the agency's commitment to maintaining only relevant and necessary PII within ITACS.
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.	The following administrative, technical, and physical controls are in place to secure PII maintained within ITACS: **Administrative Controls**: Several administrative safeguards are in place to secure PII within ITACS, including the following: User Training: All system users at the FDA are required to complete annual mandatory computer security and privacy awareness training, ensuring that all personnel with access to PII are aware of and accountable for their responsibilities in protecting the information maintained within the system. System Documentation: System documentation is in place that advises users on the proper use of the system and the handling of PII, providing clear guidance on the standards of conduct expected of all individuals who access ITACS and its PII. Need to Know and Minimum Necessary Principles:

The Need to Know and Minimum Necessary principles are applied when awarding access to the system, ensuring that access to PII is granted only to individuals with a demonstrated need to access the information in furtherance of their official duties.

Formal Supervisor Approval: FDA users, including employees and Direct Contractors, must obtain formal supervisor approval and signature before access to ITACS and its PII is granted, ensuring that access is authorized at the supervisory level.

Quarterly Access Reviews: OII conducts quarterly reviews of the system access list to adjust users' access roles and permissions and delete unneeded accounts, ensuring that access to PII remains appropriate and current.

Contractual Safeguards: Contracts with HHS/OPDiv Direct Contractors include FAR and other appropriate clauses ensuring adherence to privacy provisions and practices, providing an additional layer of administrative oversight governing contractor access to PII within the system.

Technical Controls:
Several technical safeguards are in place to secure PII within ITACS, including the following:

Multi-Factor Authentication (MFA): Access to ITACS is protected by MFA, requiring users to authenticate via a username, password, and OTP before being granted access to the system and its PII, ensuring that only authorized individuals are able to access the system.

Role-Based Access Control: Access to PII within ITACS is granted and restricted based on role-based criteria, ensuring that each user can only access the PII and system functionality that is necessary and relevant to their specific duties.

Firewalls: Firewalls are in place to protect against unauthorized access to PII within the system, helping to ensure that access is limited to only those individuals who have been properly authenticated and authorized.

Network Monitoring and Intrusion Detection Tools: Network monitoring and intrusion detection tools are in place to identify and respond to potential unauthorized access attempts or other security incidents that may affect the confidentiality, integrity, or availability of PII maintained within ITACS.

NIST SP 800-53 Controls: Additional appropriate controls have been selected from NIST's Special Publication (SP) 800-53, as determined using FIPS 199, to ensure that PII is secured in accordance with the system's level of risk and applicable federal security and privacy requirements.

Physical Controls:
The following physical safeguards are in place to secure PII maintained within ITACS:

Security Guards: All system servers on which ITACS and its PII are hosted are located at facilities protected by security guards, providing a physical layer of protection against unauthorized access to the hardware and infrastructure supporting the system.

Locked Facility Doors: All system servers are housed in facilities with locked doors, further restricting physical access to the hardware and infrastructure supporting ITACS and its PII to only authorized personnel.

Climate Controls: All system servers are located at facilities equipped with climate controls, ensuring that the physical environment in which the system's hardware and infrastructure are housed is maintained at appropriate conditions to support the continued availability and integrity of PII maintained within ITACS.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/24/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/24/2026
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:**	6/25/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 6/25/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/2/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	7

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/2/2026 2:39 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 01	BLAND, CRYSTAL	6/24/2026	6/24/2026 Per FDA's Email: The attached PIA (OII International Trade Auxiliary Communication) is SOP approved and should be in your queue for review. I have attached an exported a copy for you if you are unable to view in the HHS instance of Archer.	FW_ PTA _ PIA 5271569 is ready for APA Review.pdf 12300 OII International Trade Auxiliary Communication SOP approved.pdf