PTA / PIA: FDA - FIDA - QTR3 - 2026 - FDA5271959

Created Date: 7/10/2026 10:02 AM Last Updated: 7/10/2026 6:03 PM

General Information

PTA / PIA Name:	FDA - FIDA - QTR3 - 2026 - FDA5271959	**PTA / PIA ID:**	4626624
Component Name:	FDA - OII FDA Inventory of Data Assets	**ATO Boundary Name:**	ORA Regulatory Business Information Services
Overall Status:	Complete	**# of Days - Open:**	0
Submitter:		**Submit Date:**	7/10/2026
Next Assessment Date:	07/09/2029	**Expiration Date:**	7/9/2029
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?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	4/13/2026
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	Simmy Yau
PTA 01A:	POC Title and Organization	IT Project Manager
PTA 01B:	POC Email Address	Simmy.yau@fda.hhs.gov
PTA 01C:	POC Phone Number	703-887-7326
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 this Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA) was last approved, the Food and Drug Administration (FDA) made the following changes to the FDA Inventory of Data Assets (FIDA) system: FIDA 5.00.00 - FIDA Cloud Migration to Amazon Web Services (AWS) Government (Gov) Cloud FIDA 5.02.00 - Master Data Management (MDM) Upgrade 10.5.3 in Development (DEV), Testing (TEST), Pre-Production (PP) and Production (Prod) FIDA 5.05.02 - Update Utility (UTIL)_MAIL Oracle's Procedural Language for SQL (PL/SQL) packages in FIDA for executive order for enforced Simple Mail Transfer Protocol (SMTP) Transport Layer Security (TLS) Additionally, PTA 06 has been updated to clarify the system's record retrieval practices and their relationship to the Privacy Act determination for FIDA.
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 FDA Office of Inspections and Investigations (OII) mission is to protect consumers and enhance public health by maximizing compliance of FDA regulated products and minimizing risks associated with those products. To support this mission, OII developed FIDA to provide current, accurate, and complete firm data for workforce planning, establishing food safety policies, and the enforcement of compliance programs. FIDA serves as the authoritative master data management system for firm data at OII, helping to identify and remove duplicate firms from OII's firm inventory while also providing web services to validate addresses and match firms within that inventory. Data processed in FIDA originates from three primary sources. The first is Customs and Border Protection (CBP), a component of the Department of Homeland Security (DHS), which directs information about companies associated with imported goods subject to FDA regulation to OII for entry and storage in FIDA. The second source is Center Registration Systems (CRS), an FDA system containing firm registration information that is part of the larger FDA Unified Registration and Listing System (FURLS), which is the subject of a separate assessment. The third source is the Firm Management Services (FMS) User Interface, through which system users may directly enter new firm information if they believe a firm is subject to FDA regulation. FIDA carries out its functions through several key capabilities. These include the ability to validate United States (US) or foreign addresses, match firms based on name, address, and/or identifiers such as the FDA Establishment Identifier (FEI) number and Data Universal Numbering System (DUNS) number, validate and transfer firm data from external systems into FIDA, and share firm data — including FEI numbers, DUNS numbers, names, and addresses — with other systems. FIDA users, consisting of FDA employees and Direct Contractors, access the system via a network-level single sign-on (SSO) process using multi-factor authentication (MFA), ensuring secure and controlled access to the system. User credentials are not stored within FIDA itself; rather, they are maintained in FDA's Active Directory (AD), which serves as the authoritative system for managing user authentication and access credentials.

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.	The FIDA system collects and maintains information primarily related to regulated firms. The specific data elements collected include the FDA Establishment Identifier (FEI) number, firm name, firm physical and mailing address, firm operational status, establishment and industry type, registration number, registration status, registration date, and Dun & Bradstreet (D&B) firm name and address. While the intent of the system is to collect business information in the firm name and address fields, there are scenarios where an individual may be identified in the firm name and address. The commonly accepted scenarios in which this occurs involve clinical investigators and consignees receiving shipments who are identified as individuals rather than businesses. It is important to note that FIDA does not collect points of contact (POCs) associated with a firm. All information identified above can be shared with external OII and Center systems. FIDA records fall under National Archives and Records Administration (NARA) approved citation N-1-088-09-003, which is a Record Control Schedule (RCS). This schedule calls for the deletion of records 10 years after the final action or when no longer needed for operational, trend analysis, legal, or reference purposes, whichever is latest. In cases where data has been migrated to another system, that data would be deleted from FIDA after verification that the migration was completed successfully.
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's Active 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.	The information collected, maintained, and shared within FIDA serves the overarching mission of OII to protect consumers and enhance public health by ensuring current, accurate, and complete firm data is available for workforce planning, establishing food safety policies, and the enforcement of compliance programs. The primary intent of collecting firm name and address information is to capture business-level data; however, there are specific categories of individuals whose information may also be captured within the system as described below. Clinical Investigators are individuals who may be identified in the firm name and address fields within FIDA. Information collected about clinical investigators includes their name and business address, which is captured incidentally as part of the firm record rather than as a deliberate collection of personal information. Data pertaining to clinical investigators can be shared with other trusted FDA systems as part of FIDA's broader data sharing functions. Consignees are individuals who are receiving shipments of imported goods subject to FDA regulation. Similar to clinical investigators, the information collected about consignees includes their name and business address, which is captured within the firm name and address fields. Because there is no reliable way to distinguish consignees who are individuals from those who are businesses, their information may be shared with other systems along with other consignee records in the normal course of FIDA's data sharing operations. It is important to note that FIDA does not collect points of contact (POCs) associated with firms, and the FDA makes no secondary use of any PII that is incidentally collected within the system. All information sharing with external systems is conducted in accordance with established Information Sharing Agreements (ISAs) and other applicable data sharing agreements. Although records in FIDA may be retrieved using a firm name field that incidentally contains the name of an individual — such as a clinical investigator or consignee acting in a professional or business capacity — FDA personnel and contractors do not use PII to retrieve records in the system, as retrieval is conducted in the context of firm-level business data and the results do not constitute records about "individuals" as defined under the Privacy Act and 21 CFR Part 21.
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).	http://fida.fda.gov/bdd/

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.	FIDA is an intranet web application designed to allow FDA users to search and manage firm information, including the ability to add and update firm records within the system. The website supports OII's broader mission by serving as the primary user interface through which Official Establishment Inventory (OEI) Coordinators (District Stewards), National OEI Coordinators, and FIDA Data Quality Stewards interact with the master firm data maintained in FIDA. Each user is assigned a role within FIDA, and that role determines the scope of the user's permissions in terms of what data they are authorized to add or update within the system. Access to the FIDA intranet web application is restricted exclusively to approved FDA users, including FDA employees and Direct Contractors. The approximate number of users with access to the FIDA Informatica Data Director (IDD) user interface is 40. A person must complete an account access form, obtain proper supervisory approval, and submit the request through the appropriate channels before an account can be created. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and to delete unneeded accounts from the system. FIDA is not accessible to the general public, as it is an internally facing intranet application. The system's URL is http://fida.fda.gov/bdd/. Users access the website through a network-level SSO process using MFA, meaning users are not required to manually log into the system with a separate username and password. User credentials are maintained in FDA's AD rather than within FIDA itself, ensuring that authentication is managed centrally and securely.
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.	Biographical Information Name Contact Information Mailing Address (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	The following additional data elements are collected by FIDA and may incidentally constitute PII in scenarios where an individual is identified in the firm name and address fields: Physical Address (Business): FIDA collects firm physical addresses in addition to firm mailing addresses. In scenarios where an individual such as a clinical investigator or consignee is identified in the firm address fields, the physical address associated with that firm record may incidentally constitute PII. As with all PII in FIDA, this information is captured in the context of the individual's professional or business capacity rather than their personal capacity. FDA Establishment Identifier (FEI) Number: The FEI number is a firm-level identifier collected as part of the firm record. In scenarios where an individual such as a clinical investigator or consignee is identified in the firm name and address fields, the FEI number associated with that firm record may incidentally be linked to that individual. The FEI number is not collected as a personal identifier and is not used to identify or track individuals in their personal capacity. It is important to note that FIDA does not collect sensitive PII as defined by HHS, and the system does not collect Social Security Numbers (SSNs), Taxpayer Identification Numbers (TINs), or POCs associated with firms. Any PII that is collected is done so incidentally as part of the firm record, rather than as a deliberate effort to collect personal information about individuals. All PII collected within FIDA is limited to the name, business address, and FDA Establishment Identifier (FEI) number of individuals — specifically clinical investigators and consignees — who are identified in firm name and address fields in their professional or business capacity rather than in a personal capacity.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	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.	1,000,000 or more

PIA 25:	For what primary purpose is the PII used?	The PII maintained within FIDA is used primarily to identify individuals who are either receiving a shipment or conducting a clinical trial in their professional or business capacity. Specifically, PII may be captured for individuals who are acting as consignees — that is, individuals who are receiving imported shipments of goods subject to FDA regulation — or for individuals who are running a clinical trial in their capacity as clinical investigators. It is important to emphasize that the collection of this PII is incidental rather than intentional, as the primary purpose of the system is to collect and maintain business-level firm data in support of OII's mission. The name and business address information captured for these individuals is collected solely in the context of their professional roles and is not used to track or identify individuals in their personal capacity.
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.	FIDA's information collection and use is conducted in accordance with, and to satisfy the requirements of, numerous provisions of the following legal authorities: 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: This serves as the primary legal authority governing FIDA's information collection and use. The FD&C Act, as amended by FSMA, establishes the broad statutory framework under which FDA regulates food, drugs, and other regulated products, and within which FIDA operates to support OII's compliance and enforcement mission. 21 U.S.C. 331: This provision of the FD&C Act identifies prohibited acts related to FDA-regulated products and is among the relevant statutory provisions that govern FIDA's information collection and use in support of compliance and enforcement activities. 21 U.S.C. 350–387: These provisions of the FD&C Act cover a range of regulatory requirements related to FDA-regulated products and industries, and collectively provide additional legal authority for FIDA's information collection, maintenance, and disclosure activities in support of OII's mission to protect consumers and enhance public health.
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 Online Government Sources Other Federal Entities

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 Office of Management and Budget (OMB) information collection approval number is not required for FIDA because the system does not directly solicit or collect information from members of the public in a manner that triggers the requirements of the Paperwork Reduction Act (PRA), 44 U.S.C. 3501 et seq. The PRA applies when a federal agency conducts or sponsors the collection of information from ten or more members of the public using identical questions or reporting requirements. FIDA does not conduct such collections. Instead, the information maintained in FIDA is obtained from the following sources, none of which constitute a public information collection subject to PRA requirements: Information received from CBP and other federal government entities through existing interagency data sharing arrangements. Firm registration information received from CRS and FURLS, which are covered under their own separate privacy impact assessments (PIA) and applicable OMB approvals. Firm information entered directly by authorized FDA employees and Direct Contractors through the FMS User Interface.
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 Private Sector Within HHS

PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	FIDA shares firm data, which may incidentally include PII, with the following organizations and for the following purposes: Dun & Bradstreet (D&B) — Private Sector: Firm data is shared with D&B in accordance with executed Information Sharing Agreements (ISAs) and an agency-wide agreement governing batch feed and Integration Manager access. This sharing supports the proper identification, verification, and tracking of FDA regulated firms by associating DUNS numbers with firm records maintained within FIDA. FDA interacts with over one million business entities that manufacture, market, import, or otherwise process FDA-regulated products, and accurate tracking of these entities using unique identifiers is critical to assuring each product's safety, efficacy, and quality. Google — Private Sector: FIDA shares firm address information with Google's geo-coding application programming interface (API) in accordance with FDA's license agreement with Google, for the limited purpose of obtaining geocode values for firm addresses when FIDA's internal geo-coding service does not return results. Other FDA Centers — Other Federal Agency/Agencies: FIDA shares firm data with other FDA centers that reference firms' data in support of the broader FDA mission to ensure accurate and current firm data is available across the agency for regulatory, compliance, and enforcement purposes.

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)).	FIDA has the following agreements in place that authorize information sharing and disclosure: Google APIs License Agreement: FDA maintains an external license agreement with Google to utilize their geo-coding API. This agreement supports FIDA's Geocode Service, which is used to geocode firm addresses when FIDA's internal geo-coding service does not return values. D&B Integration Manager Agreement: FDA maintains an agency-wide external agreement with D&B for batch feed and Integration Manager access. This agreement supports FIDA's data sharing and integration processes with D&B at the agency level. FDA-DNB Information Sharing Agreement (ISA) — March 29, 2024: FDA has an external ISA with D&B, dated March 29, 2024, and expiring March 28, 2027, governing the sharing of firm data between FDA (OII FIDA) and D&B for the purpose of supporting the proper identification, verification, and tracking of FDA regulated firms. FDA-DNB Information Sharing Agreement (ISA) — May 15, 2024: FDA has a second external ISA with D&B, dated May 15, 2024, and expiring May 14, 2027, governing the sharing of firm data between FDA (OII FIDA) and D&B for the same purposes as described above.

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.	Firm data is shared between FDA (OII FIDA) and D&B in accordance with the executed ISAs and agency-wide agreements between the two organizations. Data transmissions from FDA to D&B consist of firm/facility name and address, other identifying information such as the FEI number and geocoordinates, a DUNS number along with requests for specific data elements, and other D&B-generated information based upon prior matching or address optimization conducted by D&B for firms/facilities previously submitted by FDA. Data transmissions from D&B to FDA consist of responses to queries FDA has sent to D&B, including the matching DUNS number, firm name and address as maintained by D&B, matching diagnostics including D&B Match Grades and D&B Confidence Codes, address optimization information, and D&B business intelligence information. Additionally, FIDA utilizes Google's geo-coding API in accordance with FDA's license agreement with Google to geocode firm addresses when FIDA's internal geo-coding service does not return values. All data transmissions between FDA and D&B are conducted securely through connections from FDA virtual private network (VPN) firewalls to D&B via secured Secure Sockets Layer (SSL) services, with all uniform resource locators (URLs) and Internet Protocol (IP) addresses accessible from the AWS GovCloud (US-West) environment and encrypted by the VPN tunnel.
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.	Because FIDA does not meet the definition of a Privacy Act system of records, formal Privacy Act notice and consent requirements do not apply. The PII incidentally captured within FIDA — limited to the name, business address, and associated firm identifiers of individuals acting in a professional capacity as clinical investigators or consignees — is not collected directly from those individuals, nor is it solicited for the purpose of identifying them personally. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet pages. This PIA provides further notice regarding the nature and scope of information maintained in FIDA.
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.	Formal notice and consent procedures specific to this system are not required, as FIDA does not meet the definition of a Privacy Act system of records. In the event of major changes to the system that affect information collection or use, FDA will update this PIA accordingly and publish it in accordance with applicable HHS and FDA privacy policy requirements. Updated PIAs are made available to the public on FDA.gov, providing transparency regarding any changes to the nature and scope of information maintained in FIDA.

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 many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), and other agency offices, via email, phone, and standard mail avenues (all listed on FDA.gov and the FDA intranet).
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 PII maintained within FIDA is captured incidentally as part of firm-level records rather than collected directly from the individuals to whom it pertains. Accuracy is ensured by individual review at the time of reporting, and FDA personnel may correct or update firm information as needed. PII relevancy is supported through the design of the system to require and collect only the data elements necessary to administer the system and enable its intended use. Access is granted and restricted at the individual level as appropriate to the individual's duties through role-based access controls. Integrity and availability are protected by privacy and security controls selected and implemented in the course of providing the system with an Authorization 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. FDA 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: Review and manage submissions, work planning. Administrators: Monitor the system, manage the workflow and system access. Developers: Access data for system development and maintenance. Contractors: Access data for system development and maintenance. "Contractors" here refers to FDA Direct Contractors.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory 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.	The relevant supervisor will indicate on the user account creation form the minimum access that is required in order for the user to complete their job. The scope of access is restricted based on role-based criteria.
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 Digital Transformation (ODT) verifies that individuals successfully complete the training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available via FDA's privacy office.
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).	FIDA records fall under National Archives and Records Administration (NARA) approved citation N-1-088-09-003 (a Record Control Schedule (RCS)) which calls for deletion of records 10 years after the final action or when no longer needed for operational, trend analysis, legal, or reference purposes, whichever is latest. Data migrated to another system would be deleted after verification of migration.
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 multi-factor access authentication, 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 National Institute of Standards and Technology's (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:**	7/10/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	7/10/2026
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:**	7/10/2026
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 7/10/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/10/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/10/2026 4:56 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	7/10/2026	Per FDA's Email: This PIA was recently SAOP approved (under this PIA Name **FDA - FIDA - QTR2 - 2026 - FDA5271427)** . We are resubmitting the PIA to correct an inaccuracy. This is not a Privacy Act system based on additional analysis. The PIA was updated to reflect this updated information. The PIA is experiencing an Archer error with Question #3 of the general information (Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. The ATO date is 4/13/2026 . At this time, we are unable to update Archer to reflect the correct answer “Yes.”	OII FDA Inventory of Data Assest SOP approved_updated.pdf FW_ PTA _ PIA 5271959 is ready for APA Review (resubmission).pdf