PTA / PIA: FDA - BECATS - QTR2 - 2026 - FDA5269841

Created Date: 5/29/2026 10:16 AM Last Updated: 6/18/2026 2:18 PM

General Information

PTA / PIA Name:	FDA - BECATS - QTR2 - 2026 - FDA5269841	**PTA / PIA ID:**	4532275
Component Name:	FDA - OC Biologics Export Certification and Tracking System	**ATO Boundary Name:**	OC FDA Unified Registration and Listing System
Overall Status:	Complete	**# of Days - Open:**	52
Submitter:		**Submit Date:**	5/28/2026
Next Assessment Date:	06/17/2029	**Expiration Date:**	6/17/2029
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)?	No
General 04:	ATO Date or Planned ATO Date.	7/11/2025
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	Archana Narayanaswamy
PTA 01A:	POC Title and Organization	Program Manager ODT/OIMT/OTD/DAS/EAB
PTA 01B:	POC Email Address	Archana.Narayanaswamy@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-3690
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.	Food and Drug Administration (FDA) has made no changes to this component 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 Biologics Export Certification and Tracking System (BECATS) is a web-based application operating as a component module within the Food and Drug Administration (FDA) Unified Registration and Listing System (FURLS), a major FDA application managed under the Office of Commissioner (OC) and subject of its own assessment. The Center for Biologics Evaluation and Research (CBER) utilizes OC BECATS to automate the processing and issuance of export certificates for FDA-regulated biologic products, while also providing users with the ability to track the progress of each export certificate application and electronically send notifications to users throughout the application process. The system also provides tools for FDA personnel to monitor domestic product status and identify facilities that are not in compliance with applicable laws and regulations governing the manufacturing of biologic products in the United States. OC BECATS carries out these functions through a secure, web-based interface with structured forms and integrated workflows hosted on Amazon Web Services (AWS) Federal Information Security Modernization Act (FISMA) High infrastructure. The system maintains electronic records of export certificate applications, routes submissions to FDA reviewers for processing, and facilitates secure communication between the FDA and industry users through automated electronic notifications sent throughout the application process. The legal authority for these activities is grounded in Sections 801(e) and 802 of the Federal Food, Drug, and Cosmetic Act (FD&C Act), as amended by the Export Reform and Enhancement Act of 1996, as well as Section 510 (21 U.S.C. 360) of the FD&C Act, which governs facility registration requirements for manufacturers of FDA-regulated products. OC BECATS serves two primary categories of users: external industry users and internal FDA personnel. External industry users — including both domestic and foreign facilities — access the system to submit and track export certificate applications via a publicly accessible login at https://www.access.fda.gov, authenticating through a username and password managed by the Online Account Administration (OAA) module (the FURLS user account database and user authentication module that is the subject of its own assessment). Internal FDA personnel and authorized Direct Contractors access the system to review applications, manage workflow, and monitor regulatory compliance via a network-level Single Sign-On (SSO) process using multi-factor

		authentication (MFA) tied to their existing Windows login credentials. Role-based access controls are enforced across all user types — including reviewer (RVR), scanner (SCAN), and senior reviewer (SR_RVR) roles for internal personnel — to ensure that each individual can only access the minimum amount of information necessary to perform their specific duties, in alignment with Department of Health and Human Services (HHS) privacy and security requirements.
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.	OC BECATS collects and maintains personally identifiable information (PII) about users of the application. Users include external industry users (local/foreign industry owners, operators, and agents), as well as internal FDA users (permanent employees and Direct Contractors). The PII collected from external industry users includes the following: a) first and last name; b) business mailing address; c) business phone number; d) business fax number; and e) business email address. These data elements are collected to support account creation, identity verification, and regulatory communication throughout the export certification process. Access credentials — including usernames and passwords (user credentials) — are also collected to authenticate users and manage system access. Usernames are either assigned by the system or provided by the user during account setup, and passwords are encrypted and securely stored within OC BECATS. The company taxpayer identification number (TIN) is also collected specifically from external industry users and is unique to the export certification modules within FURLS. This identifier is a company-level business identifier — not a personal one — collected as part of the account and identity information necessary to manage external user accounts. The system also maintains the following PII about internal FDA personnel and authorized Direct Contractors: a) name; b) work email address; and c) user credentials. This information is maintained within the system to facilitate role-based access and ensure that only authorized personnel can perform review and administrative functions within OC BECATS. In addition to PII, OC BECATS collects and maintains a range of non-PII necessary for regulatory oversight and certificate tracking. Facility information is collected for facilities that manufacture FDA-regulated biologic products to support regulatory oversight and compliance monitoring. Biologic product type, product code, and lot and batch information associated with export certificate applications is collected as well. Records of submitted export certificate applications are maintained within the system, as well as workflow data used track the progress of each application through the review and approval

		process. Additionally, OC BECATS generates and maintains records of electronic notifications sent to users throughout the application process, documenting communications related to submission status, required actions, and regulatory decisions. Registrants may also voluntarily submit additional non-PII data beyond what is required for mandatory submission to further support certificate processing and export tracking. PII maintained in OC BECATS is shared on a limited and controlled basis to support broader regulatory oversight functions within HHS. Within the FDA, PII is shared with the Office of Inspections and Investigations (OII), whose personnel operating the Firms Master List Service (FMLS) system have restricted read-only access to certain data tables within other FURLS modules (e.g., Food Facility Registration Module (FFRM) and Shell Egg Registration Modules). Additionally, personnel of State agencies who serve as Direct Contractors with the FDA are provided read-only access to Food Facility Registration (FFR) data to support their contracted responsibilities. Sharing is governed by the terms and conditions of Memoranda of Understanding (MOU) and Non-Disclosure Agreements (NDAs) to ensure that all recipients handle shared data in accordance with applicable privacy and security requirements. Records in OC BECATS are maintained on a temporary basis in accordance with National Archives and Records Administration (NARA)-approved retention schedules.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Username Password Non-HHS User Credentials Username Password
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	External industry users including domestic and foreign facilities that manufacture FDA-regulated biologic products are the primary category of individuals about whom PII is collected in OC BECATS. The first and last name of each external user is collected to identify the individual point of contact associated with each account and to direct regulatory correspondence to the appropriate person at a given facility. Business mailing address is collected to support written regulatory correspondence and confirm the physical location of the facility or individual associated with an export certificate application when electronic communication is not sufficient or available. Business phone number and business fax number are collected to provide FDA personnel with direct contact options for reaching industry users when

time-sensitive regulatory matters arise during the application review process. Business email address is collected as the primary channel through which automated system notifications are delivered to external industry users, including confirmations of new account creation, account deactivation or reactivation, temporary passwords for password resets, new submission confirmations, status changes, and requests for additional information.

The company TIN is collected exclusively from external industry users in connection with the export certification modules within OC BECATS. This identifier is a company-level business identifier used to verify the identity of the business entity associated with an export certificate application and to support the accurate administration of external user accounts. Access credentials — including usernames and passwords — are collected to authenticate external users and control access to the system. Usernames are either assigned by the system or selected by the user during account setup, and passwords are encrypted and securely stored within OC BECATS. Maximum lifetime restrictions are enforced on external user passwords to reduce the risk of unauthorized access through compromised credentials.

PII about internal FDA personnel and Direct Contractors is also maintained in OC BECATS. Name is maintained to identify the specific FDA employee or Direct Contractor associated with each internal user account and to support the assignment of role-based access, enabling system administrators to verify that the correct individual has been granted the appropriate level of access for their assigned duties. Work email address is maintained to facilitate internal communications related to system access administration and serves as a point of contact for the FDA Privacy Office and system administrators when resolving access-related concerns or potential privacy incidents. Access credentials are maintained to enable authentication through the network-level SSO process using MFA tied to existing Windows login credentials, supporting role-based access controls and ensuring that only authorized personnel can perform review and administrative functions within OC BECATS.

Non-PII data essential to the regulatory and operational functions of the system is collected and maintained by OC BECATS. Facility information — including facility name, registration number, establishment type, and location — is collected to identify and track facilities associated with each export certificate application and to monitor compliance with applicable manufacturing laws and regulations. Biologic product information — including product type, product code, and lot and batch information — is collected to ensure that export certificates are issued accurately and tied to the specific regulated products for which

		certification has been requested. Application submission records — including associated regulatory identifiers and tracking information — are maintained to create a complete and auditable record of each export certificate request from initial submission through final disposition. Workflow data is maintained to document the movement of each application through the stages of the review and approval process, allowing both FDA personnel and industry users to monitor submission status at any given point. System-generated notification records are maintained to preserve a complete log of all automated communications sent to users throughout the application process, providing an auditable trail of regulatory actions and decisions. PII maintained in OC BECATS is shared only to the extent necessary to support specific regulatory oversight responsibilities within HHS. Within the FDA, OII personnel operating the FMLS system have restricted read-only access to certain data tables within the FFRM and Shell Egg Registration Module to support inspection and compliance activities. Personnel of State agencies serving as Direct Contractors with the FDA are granted read-only access to FFR data solely to fulfill their contractual responsibilities. Sharing arrangements are governed by MOUs and NDAs to ensure compliance with applicable federal privacy and security requirements.
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://www.access.fda.gov
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.	The purpose of the website is to support the automated processing and issuance of biologics export certificates while providing tools for FDA personnel to monitor domestic product status and ensure that facilities comply with applicable laws and regulations governing the manufacturing of biologic products in the United States. The website serves as the primary interface through which both industry users and FDA personnel interact with the export certification process, enabling structured electronic submissions, integrated review workflows, and automated notifications that streamline certificate management and regulatory oversight. The OC BECATS website is publicly accessible with login via https://www.access.fda.gov, which serves as the entry point into the FDA FURLS platform through which OC BECATS operates. External industry users log in using username and password authentication, which is managed through the FURLS OAA module. Usernames are either assigned by the system or provided by the user during account setup, and passwords are encrypted and securely stored within OC BECATS. Internal FDA personnel and authorized Direct Contractors access the system via a network-level SSO process using MFA, which allows them to use their existing Windows login credentials to access OC BECATS and other FURLS modules without the need for separate login credentials.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	Other: fax number; User credentials include username and password; point of contact information is all business-related information.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	50,000 – 99,999
PIA 25:	For what primary purpose is the PII used?	The primary purpose of the PII collected and maintained in OC BECATS is to support account management, system authentication, and regulatory communication with industry users regarding export certificate applications, registrations, listings, and certifications.
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 legal authorities that govern information use and disclosures specific to the system and program are: The Food and Drug Administration (FDA) may issue export certificates under sections 801(e) or 802 of the Federal Food, Drug, and Cosmetic Act (FD&C Act) (as amended by the Export Reform and Enhancement Act of 1996) to facilitate export of certain regulated products. Sections 510 (21 U.S.C. 360) of the FD&C Act require domestic manufacturers, re-packers, and re-labelers (and certain foreign establishments) of human or veterinary drugs and devices to register with FDA and submit product listings, when they engage in the manufacture, preparation, propagation, compounding, or processing of such regulated products, subject to certain exemptions. For food facilities, registration is required under section 350d of Title 21. Statutory citations: 21 U.S.C. 321, 331, 342, 344, 351, 352, 355, 360, 360b, 371, 374, 381, 387e, 393; 42 U.S.C. 262, 264, 271.
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 Hard Copy Mail/Fax Email Online 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).	Form: 3613 Office of Management and Budget (OMB): Approval Number: 0910-0498 OMB Expiration Date: 06/30/2027
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.	State or Local Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Within HHS — FDA Only: OII personnel operating within the larger FURLS system boundary under which OC BECATS operates have restricted read-only access to certain data tables within certain FURLS Modules (to include OC BECATS) to support inspection and compliance activities by enabling access to facility registration data necessary for those functions. Personnel of State agencies serving as Direct Contractors with the FDA are provided read-only access to FFR data to fulfill their contracted responsibilities with the agency.
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)).	FDA establishes Memoranda of Understanding (MOUs) and employs Non-Disclosure Agreements to govern recipient data handling.
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.	All sharing arrangements are formally authorized through MOUs and NDAs, and the terms and conditions of these agreements govern the handling of shared data by all recipients.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Mandatory

PIA 33A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	The following legal authorities require individuals to provide information to the FDA in connection with the export certification and facility registration activities supported by OC BECATS: Sections 801(e) and 802 of the Federal Food, Drug, and Cosmetic Act (FD&C Act), as amended by the Export Reform and Enhancement Act of 1996, authorize the FDA to issue export certificates for FDA-regulated biologic products and establish the requirements that facilities must meet to obtain such certificates. Regulated entities that wish to export biologic products must submit the required information to the FDA as a condition of obtaining an export certificate. Failure to comply with these requirements may result in the denial of export certification and potential regulatory action. Section 510 of the FD&C Act (21 U.S.C. 360) requires domestic manufacturers, re-packers, and re-labelers — and certain foreign establishments — of FDA-regulated products, including biologic products, to register with the FDA and submit product listings when they engage in the manufacture, preparation, propagation, compounding, or processing of such regulated products, subject to certain exemptions. Failure to register as required under this section may result in civil or criminal penalties under the FD&C Act. Additional statutory citations governing information use and disclosure specific to OC BECATS include: 21 U.S.C. 321, 331, 342, 344, 351, 352, 355, 360, 360b, 371, 374, 381, 387e, and 393; as well as 42 U.S.C. 262, 264, and 271. For internal FDA personnel and authorized Direct Contractors, the submission of PII is mandatory as a condition of employment or contractual engagement with HHS/FDA. Personnel are required to provide their information in order for the agency to process administrative materials and securely administer access to agency information and systems, in accordance with applicable federal employment and contracting regulations.

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.	There is no opt-out method available for either category of users who submit PII to OC BECATS. For external industry users, including domestic and foreign facilities, there is no opt-out process for the collection or use of their PII. Regulated entities are required by law to register with the FDA and to submit the information necessary to administer the export certification process. The legal authorities governing this requirement include Sections 801(e) and 802 of the Federal Food, Drug, and Cosmetic Act (FD&C Act), as amended by the Export Reform and Enhancement Act of 1996, as well as Section 510 (21 U.S.C. 360) of the FD&C Act, which governs facility registration requirements for manufacturers of FDA-regulated products. Without the submission of required PII, the FDA would be unable to process export certificate applications, authenticate user access, or communicate with industry users regarding submission status and regulatory actions. For internal FDA permanent employees and Direct Contractors, there is likewise no opt-out option. Permanent employees, Direct Contractors, Fellows, and other personnel must provide their PII as a condition of employment or contractual engagement with the agency, in order for the FDA to process administrative materials and securely administer access to agency information and systems.

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.	If the FDA changes the collection, use, or sharing of PII data in OC BECATS, the agency will notify affected individuals by the most efficient and effective means available and appropriate to the specific change(s). The notification process differs across the two primary categories of individuals whose PII is maintained in the system: For external industry users, including domestic and foreign facilities, notification of major changes to the system's privacy practices or data collection, use, or sharing will be provided through electronic means, including email notice sent directly to the affected individuals using the business email addresses maintained in OC BECATS, and/or through a prominently posted notice on the FDA website at fda.gov. Additionally, the FDA's privacy policies are permanently posted on fda.gov, and any updates to those policies will be reflected there in a timely manner. External users may also be notified through formal written correspondence where appropriate to the nature and significance of the change. For internal FDA personnel and Direct Contractors, notification of major changes will be provided through agency-wide communications, including email notices to affected individuals, information provided to supervisors with instructions to further inform staff, inclusion in agency newsletters or intranet postings, and privacy awareness events and workshops held within the FDA. The FDA Office of Digital Transformation (ODT) and the FDA Privacy Office will coordinate the dissemination of such notifications to ensure that all affected internal personnel are informed in a timely manner. Regarding consent, because the submission of PII in OC BECATS is mandatory for external industry users — as governed by the legal authorities — obtaining affirmative consent from individuals as a precondition of continued system use may not be practicable in all circumstances. However, the FDA is committed to transparency in its privacy practices and will make every effort to inform affected individuals of any material changes to the collection, use, or sharing of their PII through the notification methods described above. No changes that would materially affect the rights or interests of individuals are currently anticipated.

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. External individuals may contact FDA offices, including the Privacy Office and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov). In addition to those resources identified for external individuals, internal FDA users may also contact the Employee Resource and Information Center (ERIC), and the FDA Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). FDA personnel are required to rapidly report any suspected incidents or breaches to the FDA CIOCC.

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.	PII maintained in OC BECATS is self-submitted by registrant points of contact, who certify the accuracy of the information provided at the time of submission. External industry users may correct or update their PII directly within the FURLS platform at any time using their authenticated account access, or by contacting the FDA using the contact information provided on fda.gov. For internal FDA permanent employees and Direct Contractors, PII may be corrected or updated directly within the system or through the relevant system administrators or the FDA Privacy Office. The relevancy of PII is supported through the system's design, which collects only the data elements necessary to administer the system and enable its intended use. Role-based access controls ensure that each individual can only access the minimum amount of information necessary to perform their specific duties. The agency reviews the system access list on a quarterly basis to adjust permissions and remove unnecessary accounts and certificate module records are deleted and destroyed in accordance with NARA retention schedules. The integrity of PII is protected by administrative, technical, and physical controls selected and implemented in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and appropriate to the system's High impact security categorization as determined using NIST Federal Information Processing Standards (FIPS) 199. Technical safeguards include MFA, firewalls, and network monitoring and intrusion detection tools. Annual mandatory computer security and privacy awareness training for all system users further supports the integrity of PII by ensuring that personnel understand their responsibilities for protecting information maintained in OC BECATS. The availability of PII is protected by the same comprehensive set of security controls implemented as part of the system's Authorization to Operate (ATO) process. OC BECATS operates as a component of the FURLS platform, hosted on AWS FISMA High infrastructure and accessible 24 hours a day, 7 days a week, 365 days a year. Physical controls — including security guards, locked facility doors, and climate controls — further support system availability. Akamai caching services optimize routing and ensure the system remains responsive to authorized users. Business continuity and contingency planning measures are maintained in accordance with NIST SP 800-34 to ensure prompt restoration of the system in the event of an outage or disruption.

PIA 38:	Identify who will have access to the PII in the system.	Users Administrators 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: Internal FDA personnel, including permanent agency employees, require access to PII maintained in OC BECATS to perform their regulatory oversight responsibilities. This includes the ability to receive, review, manage, and track export certificate applications submitted by industry users, as well as to communicate with industry users regarding submission status and regulatory actions. FDA personnel are assigned specific roles — such as reviewer (RVR), scanner (SCAN), and senior reviewer (SR_RVR) — that define the scope of their access within the system and ensure that each individual can only access the minimum amount of information necessary to perform their specific duties. Internal FDA personnel access the system via a network-level SSO process using MFA tied to their existing Windows login credentials. External industry users, including domestic and foreign facilities, have access to their own PII maintained in OC BECATS for the purpose of submitting and managing export certificate applications. External users can create their own accounts, submit and track export certificate applications, and update their own account information as needed. Their access is strictly limited to their own account information and submission data, and they are not permitted to access the PII or submission data of other users. External industry users access the system via username and password authentication managed through the FURLS OAA module, with usernames either assigned by the system or provided by the user during account setup and passwords encrypted and securely stored within OC BECATS. Administrators: System administrators require access to PII maintained in OC BECATS to perform essential administrative functions necessary for the operation and maintenance of the system. These functions include conducting annual access reviews and updates, activating or reinstating canceled facility registrations, resetting user passwords, and managing user accounts. A subset of these administrators are Direct Contractors who perform administrative functions under their FDA contract. Administrator access is granted based on supervisor approval and is subject to the Need to Know and Minimum Necessary principles, ensuring that administrators can only access the PII necessary to perform their specific administrative duties.

Contractors: Authorized Direct Contractors require access to PII maintained in OC BECATS to fulfill their responsibilities under their FDA contracts. Contractor access is generally limited to read-only mode, ensuring that contractors can view the data necessary to perform their contracted responsibilities without the ability to modify or delete PII. All contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices. Contractors are required to safeguard all information handled in connection with their FDA contract and to report potential data breaches to the FDA promptly.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Internal FDA personnel and Direct Contractors who require access to OC BECATS must obtain supervisor approval before access is granted. The requesting user's supervisor reviews the access request and uses an account creation form to specify the minimum application access required for the user to perform their specific job duties, in alignment with the Need to Know and Minimum Necessary principles. The scope of access awarded to each internal user is determined by their assigned role within the system which defines the functions they are permitted to perform and the information they are permitted to access within OC BECATS. Role-based access controls are enforced across all internal user types to ensure that each individual can only access the minimum amount of PII necessary to perform their specific duties. All internal users are required to complete annual mandatory computer security and privacy awareness training, as verified by the FDA ODT, before access is granted and on an ongoing basis thereafter. The agency reviews the system access list on a quarterly basis to review and adjust user access permissions and to remove unnecessary or inactive accounts from the system, ensuring that access remains appropriate to each user's current role and responsibilities. Direct Contractors are subject to the same supervisor approval and role-based access control procedures as internal permanent FDA personnel. All contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices, and contractors are required to safeguard all information handled in connection with their FDA contract. Access for external users is strictly limited to their own account information and submission data, and they are not permitted to access the PII or submission data of other users. External user accounts are reviewed on a quarterly basis, and inactive accounts are deactivated to minimize the risk of unauthorized access. Additionally, maximum lifetime restrictions are enforced on external user passwords to further support the security and integrity of external user access.

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.	OC BECATS employs a comprehensive set of technical network and application security controls to protect PII and enforce minimum necessary access. These include firewalls and network monitoring and intrusion detection tools that detect and respond to unauthorized access attempts and other potential security incidents. Services also include caching services that optimize routing and ensure that users requesting web pages with dynamic content or sensitive data are routed directly to the FDA FURLS servers, further protecting PII from unauthorized interception or access. Technical account management controls are in place to ensure that access to PII remains limited to active and authorized users at all times. External user accounts are reviewed on a quarterly basis, and inactive accounts are automatically deactivated to minimize the risk of unauthorized access by former or inactive users. Additionally, accounts expire after 90 days of inactivity for external users, providing a technical mechanism to enforce the removal of access for users who are no longer actively engaging with the system. All user passwords are encrypted and securely stored within OC BECATS, ensuring that access credentials cannot be accessed or exploited by unauthorized individuals. The system employs encryption and other data protection measures in accordance with NIST Special Publication 800-53 security controls and Federal Information Processing Standards (FIPS) 199, appropriate to the system's High impact security categorization, to protect PII both at rest and in transit.
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 internal FDA personnel who access OC BECATS including system owners, managers, operators, program managers, and Direct Contractors are required to complete annual mandatory computer security and privacy awareness training as a condition of continued system access. The FDA Office of Digital Transformation (ODT) verifies successful completion and maintains certificates of completed training for all FDA employees and Direct Contractors, providing an auditable record of training compliance. The annual training covers federal laws, policies, and regulations relating to privacy and data protection, including the Privacy Act of 1974 and the Federal Information Security Modernization Act (FISMA); the proper handling of PII and any special restrictions on data use and disclosure applicable to OC BECATS; the identification and reporting of suspected privacy incidents and data breaches to the FDA Cybersecurity and Infrastructure Operations Coordination Center (CIOCC); the application of the Need to Know and Minimum Necessary principles when accessing and handling PII; and the HHS Rules of Behavior, which establish the standards of conduct expected of all individuals who access HHS information systems.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to the annual mandatory training described, OC BECATS system users receive supplemental training and guidance. Internal FDA personnel and Direct Contractors receive system-specific training on the FURLS platform and OC BECATS module, covering the submission, review, processing, and tracking of export certificate applications, as well as the role-based access controls enforced within the system. Personnel assigned specific roles receive role-specific guidance on the scope of their access and the functions they are permitted to perform. All system users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving OC BECATS. Internal users of the application also have access to supplemental privacy program materials available on a central FDA intranet page and may contact the FDA Privacy Office for additional guidance. Information security and privacy awareness events and workshops held within the FDA provide further opportunities for personnel to stay current on emerging privacy and security topics and updates to applicable federal laws and FDA policies. External industry users are provided guidance on the FDA's privacy practices and proper system use at the time of account creation, through the privacy notice posted at https://www.access.fda.gov, and through privacy policies permanently posted on fda.gov.

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 following NARA-approved records retention schedules apply to PII and other information maintained in OC BECATS: FDA File Codes 7210 and 7222 — Registration and Listing files and system database records, covered under NARA-approved citation N1-88-07-2, Item 6.1. Records covered under these file codes are considered temporary and are cut off after an establishment goes out of business or a product is no longer commercially marketed. Certificate Module Records — OC BECATS Specific — Records maintained in the OC BECATS certificate module, which directly apply to the export certification activities supported by OC BECATS, are deleted and destroyed after five years following the applicable cutoff date. This five-year retention period is specific to the certificate modules within FURLS, of which OC BECATS is one, and reflects the temporary nature of export certificate application records following the cessation of the associated regulatory activity. FDA File Codes 7220-7225 — Registration and Listing Systems records, covered under NARA-approved citation N1-88-07-2, Item 6.1. Records covered under these file codes are considered temporary and are destroyed when no longer needed, when the establishment goes out of business, or when the product is no longer marketed, with a maximum retention period of ten years after cutoff or when no longer needed for legal, research, historical, or reference purposes, whichever is latest. The destruction of PII and other records maintained in OC BECATS is carried out in accordance with FDA records management policies and applicable NARA regulations. Administrative safeguards, including system documentation and records management procedures, govern the identification and scheduling of records eligible for destruction. Technical safeguards, including secure deletion tools and database management procedures, are employed to ensure that electronic records are destroyed in a manner that prevents unauthorized recovery or reconstruction of destroyed PII. Physical safeguards are applied to any physical records or media containing PII to ensure their secure destruction in accordance with applicable federal standards.

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 annual mandatory computer security and privacy awareness training for all system users, verified and tracked by FDA ODT. Access is governed by the Need to Know and Minimum Necessary principles, with supervisor approval required before access is granted. System manuals and documentation advise users on the proper use of OC BECATS and applicable security and privacy requirements. The agency reviews the system access list on a quarterly basis to adjust permissions and remove unnecessary or inactive accounts. All contracts include Federal FAR clauses ensuring adherence to privacy provisions and practices. Technical safeguards include MFA for internal users via SSO, and username and password authentication for external users managed through the FURLS OAA module, with passwords encrypted and securely stored. Role-based access controls (RBAC) are enforced across all user types to restrict access to the minimum information necessary. Firewalls, network monitoring, and intrusion detection tools are in place to detect and mitigate application layer attacks. Security controls have been selected from NIST Special Publication 800-53, appropriate to the system's High impact security categorization as determined using FIPS 199. All system servers are located at secure facilities and hosted on Amazon Web Services (AWS) FISMA High infrastructure, protected by security guards, locked facility doors, climate controls, and robust physical security measures maintained in accordance with the stringent requirements applicable to FISMA High federal information systems.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/28/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/29/2026
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. Note the Archer error associated with question General 03: "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. At this time, we are unable to update Archer to reflect the correct answer "Yes." The ATO date is 7/11/2025. The FDA Archer Team is aware of this occurrence and is working on a solution.	**# of Days - SOP Review:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/15/2026
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/15/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	17

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/18/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/18/2026 1:36 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 09	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 22	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 22A	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 25	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 27	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 32D	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 33A	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 34	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 35	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 36	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 37	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	
PIA 40	Data Feed Service, pta_pia_FDA_Release	5/28/2026	Addressed	