PTA / PIA: FDA - OLTS - QTR3 - 2025 - FDA4956264

Created Date: 9/11/2025 12:25 PM Last Updated: 9/17/2025 4:33 PM

General Information

PTA / PIA Name:	FDA - OLTS - QTR3 - 2025 - FDA4956264	**PTA / PIA ID:**	3780294
Component Name:	FDA - OII LearnED Training System	**ATO Boundary Name:**	OII LearnED Training System
Overall Status:	Complete	**# of Days - Open:**	12
Submitter:		**Submit Date:**	9/10/2025
Next Assessment Date:	09/16/2028	**Expiration Date:**	9/16/2028
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?	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.	12/16/2022
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	POC Name: La'Wanda Giles
PTA 01A:	POC Title and Organization	Management Analyst - Acting Team Lead OII/OTED/Division of Instructional Systems and Technology
PTA 01B:	POC Email Address	lawanda.giles@fda.hhs.gov
PTA 01C:	POC Phone Number	301-529-5137
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 URL changed as a result of Cornerstone migrating to Amazon Web Services.
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 purpose of the OII LearnED Training System (previously known as "Cornerstone Learning Management System") is to provide a system that collects and maintains training data for FDA, State, Local, Tribal, and Territorial personnel such as course completion dates and incomplete status data. The system supports the administration, documentation, tracking and reporting of FDA-specific training programs, classroom and online events, online programs, and training content. It provides tools to manage training programs as well as a central repository for online training and automation of administrative tasks.
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 system maintains training information and associated personally identifiable information (PII) about: current and past OII employees who are required to or have completed training; State, Local, Tribal, and Territorial officials and Direct Contractors who are required to or have completed training; and, the supervisors of individuals required to or who have completed training. The only individuals who can access the OII LearnED Training System are FDA employees, Direct Contractors, other federal government users approved by FDA to take FDA courses, and State, Local, Tribal and Territorial employees under contract to perform duties on behalf of FDA and approved by FDA as OII Learned users. State, Local, Tribal and Territorial organizations and employees have entered into contractual and/or cooperative agreements with the FDA to conduct inspections on behalf of the agency. These relationships enable the FDA to provide training to prepare individual sot conduct inspections and to assist jurisdictions in gaining the appropriate infrastructure, which includes training, as a means to comply with the Manufactured Food Regulatory Program Standards and achieve the agency's goal of an Integrated Food Safety System. Information and data elements collected into and maintained in the system include: learner name, position, title, grade, duty station, business phone number, fax number, work email address, supervisor's name, supervisor's work phone number, certificates and education records, and individuals' organization identifiers such as an FDA Enterprise Administrative Support Environment (EASE) ID, organization type (State, Local, Local/County, Tribal, Territorial), agency name, Occupational Series Code, supervisory status, and location (State/Territory). Once approved, State, Local, Tribal and Territorial users and federal government users access the system using an assigned username and a temporary password provided to them via e-mail (user credentials).

		Users can reset their temporary password to a password of their choosing that meets complexity standards. FDA learners (permanent employees and Direct Contractors) use a Single Sign-On (SSO) process with two-factor authentication to access the system rather than a system-specific password and username. Other data in the system include: course feedback and ratings, course overviews, course content, course description, course objectives, target audience, scores, right/wrong answers, registration date, course name, course code, completion date, pass/fail outcomes, completion status, course dates, continuing education units (CEUs), contact hours, seat capacity, pre-requisites, class status, division, course instructor name, completion certificates, communications, email with students and instructors, user-controlled profile information, and course materials. In addition, there is a Knowledge Bank for User Guides and Job Aids, and voluntary Communities are available for users to ask and answer questions about the system.
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 Non-HHS User Credentials Username Email Address
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 LearnED Training System is a licensed product of Cornerstone-on-Demand (CSOD), a software application for the administration, documentation, tracking and reporting of FDA-specific training programs, classroom and online events, online programs, and training content. It provides tools to manage training programs. It provides a central repository for online training and automates administrative tasks. The system maintains data related to instructor-led sessions, individual course completions, online course completions, certifications, and transcript information. The OII Office of Training, Development and Education (OTED) is a primary provider of training and development for FDA, State, Local, Territorial, and Tribal regulatory officials. Only FDA employees, Direct Contractors, State, Local, Tribal, and Territorial (SLTT) employees, and other Federal government users approved by FDA to take FDA courses are authorized to log into OII LearnED and register for courses. FDA users (FDA employees or Direct Contractors who are learners or administrative users) authenticate via SSO using their FDA personal identity verification (PIV) card and associated credentials. The system maintains the training history for FDA personnel and a limited scope of personally identifiable information (PII) obtained from the Enterprise Administrative Support

		Environment (EASE), which is another internal FDA system and assessed in a separate PIA) consisting of each employee learner's (a) first and last name; (b) FDA e-mail address; (c) Enterprise Administrative Support Environment (EASE, the subject of a separate assessment) identification number; and (d) FDA Center name and/or organization acronym for FDA employees and Direct Contractors. The system also holds learner name, position, title, grade, duty station, business phone number, fax number, work email address, supervisor's name, supervisor's work phone number, certificates, and training records. State, Local, Tribal, Territorial, Contractor, and other non-FDA government end users (learners) gain access to the system with a unique Login ID and password. The password is created and controlled by the user and can be reset by the user. OII LearnED Training System administrators review and approve/deny each account request. State, Local, Tribal Territorial, Contractors, and other non-FDA government employees request an account in OII LearnED by filling out an online self-registration request form. This form includes name, position title, work email address, organization, employer type, work location, business phone number, manager's name, manager's email address, county, Tribe and agency. At their option, the user may include previous email addresses, previous names, and previous agencies to help avoid duplicate account creation. Upon Administrator approval and account creation, a User ID is automatically created by the system, based on the user's email address. The system retains the same PII for all users and administrators of the system, whether learner, instructor, current or former employee, administrator, or current or former State/Local/Tribal/Territorial partners. Administrative users of the LearnED Training System retrieve information from the system about all users by utilizing the following PII: user last name, user unique ID, or user email address.
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://fdaoted.csodfed.com/
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.	This is a publicly accessed URL. However, it is the front facing login page that requires a username and password or Single Sign-On (SSO) authentication for FDA users. It is used for internal FDA users as well as external State, Local, Tribal and Territorial users.
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?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
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 Persistent 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 User Credentials Certificates (e.g., training certificates) Education Records Employment Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) 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.	Individuals’ organization identifiers such as an FDA Enterprise Administrative Support Environment (EASE) ID
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

PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	5,000 – 9,999
PIA 25:	For what primary purpose is the PII used?	PII in the system is used to control system access and communicate with and identify users. Contact information will routinely be used to coordinate training. Addresses will be used to send training material. Job titles will be used for suggestions of courses. PII is also used for knowledge sharing and collaboration within the system as well as user provision of feedback (e.g., ratings and comments) regarding training courses and system functionality, which may include question-and-answer activities. Users' names are associated with these system uses. FDA employees may search for an FDA employee by name. This will bring up a Bio page with employee name, Organization acronym, Occupational Series, work phone, email address, work location, position title, and team members. The purpose of this is to be able to connect with other users of the system. This option is not available for State, Local, Tribal or Territorial users. End users also have the option of participating in voluntary Community discussions, to ask and answer questions regarding the functionality of the system. Users' names are associated with the questions and answers. Users also have the opportunity to voluntarily assign star ratings and comments for courses they have completed in the system. Users' names are associated with the ratings and comments. A knowledge bank of user guides and Job Aids is also available.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	FDA makes no secondary uses of PII handled in the OII LearnED Training System.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Executive Order 11348, 44 U.S.C. 3102, and generally 5 U.S.C. 4101 and 4118, and 44 U.S.C. 2901 and 2904.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	Last name, Unique ID, or email address of students (users)
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	SORN 1: OPM GOVT-1 General Personnel Records SORN 2: HHS SORN 09-40-0001 Public Health Service (PHS) Commissioned Corps General Personnel Records

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV State/Local/Tribal Other
PIA 30A:	Identify the "other" sources of PII in the system not mentioned in the above list.	Enterprise Administrative Support Environment
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.	This system/component does not collect information using an information collection request as defined by the Paperwork Reduction Act.
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.	Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	The system provides EASE ID to the contractor personnel operating the system (The Educe Group and Cornerstone on Demand) to provide access to the system for all FDA employees and Direct Contractors required to take the courses the system hosts.
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)).	Contractor access to information is addressed in the contract between FDA and The Educe Group as well as signed Non-Disclosure Agreements between the FDA and all contractor personnel with access to EASE data. Direct Contractors are required to adhere to the same laws, regulations, policies, and procedures as permanent employees. Both Direct Contractors and permanent employees are subject to civil and criminal penalties, including the criminal penalty provisions of the Privacy Act, applicable in the event of violations.
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.	If records in the system are shared outside of HHS, the Records Management team will maintain a listing of disclosures for which an accounting is required pursuant to the Privacy Act, 5 U.S.C. 552a(c). Note that under FDA regulations and Federal court decisions, contractor personnel operating this system on behalf of the FDA are considered agency employees and therefore the accounting requirement does not apply to disclosures to employees of the contractor operating this system.
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.	While the collection is "voluntary" in the sense that supplying it is not required by statute, individuals must supply PII as a condition of employment. There is no opt-out of the collection of PII. The training provided through the system is typically mandatory and the work-related PII is needed to maintain each individual's training status and to notify them when it is necessary to complete the mandatory training.
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.	FDA does not anticipate any major change that would affect individuals' privacy. In the event of a major change, the agency will notify individuals whose PII is in the system by the most efficient and effective means available and appropriate to the specific change(s). This may include a formal process involving written and/or electronic notice such as additional or revised privacy notices and/or Privacy Act Statements provided within the system and the online course materials, or informal processes such as e-mail notice to the individuals.
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.	Much of the PII in the system is about FDA personnel and Direct Contractors supplied by FDA's EASE system and in many cases, personnel may access their EASE data on their own to update or correct their information. Individuals may also contact the FDA's Privacy Office, their Information System Security Officer, or FDA's Employee Resources and Information Center (ERIC) to seek assistance with any PII use or disclosure concerns or to correct inaccurate information. Many of these resources are available to external individuals as well. Both internal and external individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have many options available for assistance. These individuals may contact FDA offices, including the FDA Privacy Office, the Employee Resource, and Information Center (ERIC, a resource for FDA personnel), Cybersecurity and Infrastructure Operations Coordination Center (CIOCC, responsible for receiving reports of information incidents from FDA personnel) and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel and Direct Contractors must report that without delay to the FDA's 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.	Data is refreshed on a nightly basis to ensure data accuracy and relevancy. The system is designed to collect only that PII which is necessary for the purpose of the system. The system is audited in accordance with FDA IT security requirements to protect the integrity and availability of the system.

PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	Third-Party Contractor (Contractors other than HHS 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 personnel (employees, Fellows, Direct Contractors) have access to their individual PII information to review/update it and observe training history and status. FDA personnel also have access to the PII of other FDA personnel in certain contexts as described elsewhere in this assessment such as when participating in course feedback activities and user collaborations. For external users (e.g., State, Tribal, Territorial), system administrators review and approve/deny each account request. Administrators: Manage the system, control access, help desk support and completion reports. Developers: System maintenance and enhancement Contractors: Project Management and system administrators (Help Desk): includes Third Party contractors from the Educe Group and software vendor Cornerstone on Demand.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Supervisors review all system access requests and ensure that Center/Office Administrators have access only to the relevant individual's (user) name, FDA e-mail address, office name, and course completion status. Likewise, for external users (e.g., State, Local, Tribal, Territorial), system administrators review and approve/deny each account request.
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.	Supervisory review of system access requests is required and ensures that Center/Office Administrators have access only to the relevant user's name, FDA e-mail address, office name, and completion status. For external users (e.g., State, Local, Tribal, Territorial), system administrators also review and approve/deny each account request. Access is controlled at the individual level via technical settings and system controls based on roles and responsibilities (enforcing least access and need-to-know).

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.	The FDA makes it mandatory for all FDA personnel, Direct Contractors and other individuals with access to PII about others to complete information security and privacy training every year. A portion of this training is dedicated to the protection and use of PII.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Users are provided a link to the FDA's Rules of Behavior and privacy policy. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA. Privacy guidance is also available via the 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).	Records are managed in accordance with General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001, Disposition: TEMPORARY. records may be destroyed 1 year(s) after the system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. National Archives & Records Administration (NARA) N1-088-08-003, Item 1.1.1. FDA File Code 4911 covers FDA-Wide Training Program (Mission Areas) Course Materials, Disposition: TEMPORARY. Cutoff at the end of the fiscal year when obsolete or superseded. Delete or destroy 20 years after cutoff or when no longer needed for reference, whichever is later. NARA GRS 2.6, Item 030, FDA File Code 4925 covers FDA Employee/Direct Contractor Individual Training Records, Disposition: TEMPORARY. Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use.

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.	FDA applies administrative, technical, and physical security controls consistent with National Institute of Standards and Technology (NIST) guidance. 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. The system is also required to complete the Authority to Operate (ATO) process, which includes a thorough consideration of security controls. A couple of examples of rigorous security practices follow. The application is entirely rights and roles driven. General rules are established for certain types of administrators, and each user may also be granted their own unique permissions. These permissions are all stored as part of the user's information. The system also has multiple types of encryptions ensuring that data is protected both at rest and while in transit. This ensures that the databases and all associated files are encrypted at rest, including any backups written to disk as well as the transaction logs. The application also encrypts data in transit. The certificate used to encrypt the FTPS (File Transfer Protocol with Transport Layer Security) traffic is issued from a publicly trusted certificate authority.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/11/2025
Privacy Analyst Review Comments:	The PIA is experiencing an Archer error 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. The ATO date is 12/16/2022. At this time, we are unable to update Archer to reflect the correct answer “Yes.”	**# of Days - PA Review:**	1

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	9/11/2025
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:**	9/12/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 9/12/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	9/17/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	5

SAOP Signature

Date	User	Type	Name	Original Value	New Value
9/17/2025 2:38 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	9/11/2025	Per FDA's Email and Attachment: Note the Archer error associated with question General 03: “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” o The FDA instance of Archer is automatically entering the answer “No” which is incorrect. o At this time, we are unable to update Archer to reflect the correct answer “Yes.” The ATO date is 12/16/2022. The FDA Archer Team is aware of this occurrence and is working on a solution.	OII LearnED Training System_SOP Approved.pdf 9-11-2025 EMAIL_FDA (OII LearnED Training System) PTA _ PIA 4956264.pdf