PTA / PIA: FDA - CSA - QTR3 - 2025 - FDA4950091

Created Date: 8/11/2025 4:43 PM Last Updated: 8/13/2025 12:43 PM

General Information

PTA / PIA Name:	FDA - CSA - QTR3 - 2025 - FDA4950091	**PTA / PIA ID:**	3635053
Component Name:	FDA - CDRH Salesforce Applications	**ATO Boundary Name:**	CDRH Center Engagement and Workforce Development
Overall Status:	Complete	**# of Days - Open:**	2
Submitter:		**Submit Date:**	8/11/2025
Next Assessment Date:	08/12/2028	**Expiration Date:**	8/12/2028
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?	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.	8/18/2023
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	POC Name: Dawn Stephens
PTA 01A:	POC Title and Organization	POC Title: Division Director POC Organization: CDRH/OSPTI/OTDS/DTS
PTA 01B:	POC Email Address	dawn.stephens@fda.hhs.gov
PTA 01C:	POC Phone Number	3018303377
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.	FDA has made no changes to this CDRH Salesforce Applications since the last Privacy Threshold Analysis/Privacy Impact Assessment 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 Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) salesforce Applications system ("CDRH salesforce" or "salesforce" or "salesforce Applications") is a Platform-as-a-Service (PaaS) / Software-as-a-Service (SaaS) cloud environment designed to host and easily deploy a variety of different workflow, business management and regulatory support applications. FDA/CDRH data resides in logically separated domains enabling FDA/CDRH to maintain complete and native control over all data stored and processed within Salesforce. This system is used by FDA/CDRH employees and their customers, (e.g., FDA employees who are not system users, Medical Device Companies, charities, educational institutions, medical institutions). The FDA (internal) customers include: Office of Communication and Education (OCE), Office of Science and Engineering Laboratories (OSEL), Division of Industry and Consumer Education (DICE), Digital Health Center of Excellence (DHCoE) and users of the following CDRH projects: Unique Device Identification (UDI), Critical Path, Payor, and the 506J project team. Salesforce allows the internal FDA Salesforce users to respond to these emails, sort and file them with various views, and run metrics (for example, seeing how many emails of a particular type were submitted in the last 90 days, or how long on average it takes an internal FDA user to respond to specific types of emails). External customers utilizing Salesforce applications are medical device manufacturers seeking to communicate and provide information to CDRH via the external-facing elements of the system, speakers for OCE events, and entities applying for a universal device identifier (UDI) Data Universal Numbering System (DUNS) number (a proprietary nine-digit business identifier issued by the private sector company, Dun and Bradstreet). This privacy impact assessment (PIA) addresses the underlying platform and specific applications that FDA operates using the platform. FDA conducts additional separate assessments of other applications that agency programs operate in (developed and/or hosted in) the Salesforce environment. FDA's use of the underlying platform of Salesforce Applications does not require and is not intended to entail the collection or use of personally identifiable information (PII) or other data. The company's employees email address is captured, as well as the subject and body of said email/question/request). A company's employee sends an email to an official FDA email address,

		which is then automatically forwarded into Salesforce. Salesforce then creates the email into a case, capturing the email address and the subject matter of the email. Internal FDA Administrative Portal - The internal portal is accessed by internal FDA employees only and supports a variety of configurations. The Internal Administrative Portal provides Helpdesk functionality which enables internal users to manage incoming inquires. Inquiries are service requests received from external entities, ranging from asking a question to submitting a request to be processed by the specific branch. CDRH uses the administrative portal to organize and manage incoming cases and requests to better serve both sides of the process. FDA internal webforms: CDRH Critical Path project users currently utilize the internal webform within Salesforce to manage the submission from internal employees in order to help gauge/handle and administrate ideas from FDA employees and process funding requests for said proposals. FDA external webforms: The webforms below provide external users the ability to submit inquiries to CDRH. All webforms are unauthenticated and do not share/expose any data with/to the external user and are accessible through via FDA.gov. Submitted forms are saved internally in Salesforce. Users with internal FDA Salesforce access and express permissions can access the internal side of Salesforce. Specific uses: CDRH 506J webform is used for collecting information on shortages of medical devices. CDRH Unique Device Identification (UDI) webform is used for Global Unique Device Identifier Database (GUDID) questions and requests. CDRH Office of Communication and Education (OCE) Speaker Request webform provides internal users with the ability to manage requests for CDRH speakers at events. Access to the Salesforce system is through a single sign-on (SSO, only for FDA users with a Salesforce license) multifactor authentication process, and access to the webform link is through the web browser. Credentials for FDA system users are stored within Salesforce and FDA users are required to be connected to the FDA network. External users with non-FDA credentials, access the webform link via the web browser (no credentials required).
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.	CDRH SalesForce is a Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) cloud environment capable of hosting low or moderate sensitivity/impact data including PII of such

sensitivity. Designated application owners within CDRH are responsible for the PII and any other data that is collected, stored, displayed and/or transmitted in their use of the FDA's CDRH Salesforce environment.

CDRH Salesforce is a system that collects the following information for the purpose of employing various applications desired to support various CDRH missions.

The Internal FDA Administrative portal collects the following PII about OSEL, DICE and Payor users: (a) company/work email. It also collects the following PII about DHCoE users: PII (a) company/work email; and (b) first name/last name; (c) owner email (business owner); (d) internal record owner (FDA Direct Contractor's name); and (e) user credentials.

The Internal FDA Administrative portal collects the following non-PII information from OSEL users: (a) title; (b) status, (c) description; (d) department/lab; (e) office/program; and (f) email origin. In some instances, it may be possible to combine data elements to identify an individual.

The portal also collects the following non-PII information from DICE users: (a) email subject; (b) spam; (c) attachment checkbox, (d) manager comments; (e) date opened/closed; (f) prior case; (g) ombudsman's list; and (g) response due date.

The portal also collects the following non-PII information from Payor users: (a) case number; (b) organization name; (c) device name; (d) date/time opened; (e) status; (f) sub-status category; (g) linked submission; (h) calendar date of contact; (i) email subject; and (j) current pre-sub meeting date.

The portal also collects the following non-PII information from DHCoE users: (a) status/subject; (b) internal case owner, (c) date and time opened/closed; (d) case origin; (e) prior case; and (f) internal/external contact.

The FDA internal webform collects the following PII about CRDH Critical Path users: (a) company/work email; (b) supervisor name; (c) supervisor email. The webform also collects the following non-PII information from CRDH Critical Path users: (a) proposal title; (b) status; (c) application status; (d) date/time opened; (e) office; (f) position/title; (g) summary; (h) regulatory science priority; (i) evidence of regulatory science gap; (j) value proposition; (k) public health impact; (l) progress to date; (m) specific aims; (n) research strategy; (o) additional information; (p) references; (q) level four research imperatives; (r) level three internal outputs; (s) level two external impacts; (t) outcomes for evaluating impact; (u) center rating; (v) awarded amount; (w) center rating notes; (x) total rating cost; (y) total supplies cost; (z) total

		project cost; and (aa) budget justification. CDRH 506J webform collects the following PII information: (a) company/work email; (b) company name; (c) first name/last name; and (d) work phone number; (e) FEI number; and (f) UDI number. CDRH 506J webform also collects the following non-PII information: (a) notification type; (b) product code; (c) marketing submission holder; (d) submission number; (e) device trade name; (f) model number; (g) SKU number; (h) notification status; (i) pediatric device (yes/no); (j) interruption reason; (k) estimated duration of interruption; (l) impact of COVID-19 on distribution and manufacturing; (m) reliance on critical suppliers (yes/no); (n) device made on multiple facilities; (o) has the shortage been publicly announced; (p) input on preventing future interruptions; (q) estimated market share impacted by COVID-19; (r) average historical production in the US; (s) current production; (t) current US distribution; (u) max production; (v) current inventory; and (w) reason no notification is needed. CDRH UDI webform collects the following PII (a) company/work email; (b) first name/last name; (c) company phone number; and (d) DUNS number. CDRH UDI webform also collects the following non-PII information: (a) organization name; (b) organization type; (c) subject; and (d) type of question. CDRH OCE Speaker Request webform collects the following PII information from OCE users: (a) company/work email; (b) first name/last name; (c) work phone number; (d) sponsor first/last name; (e) sponsor phone number; (f) sponsor email; (g) speaker first/last name; and (h) speaker branch/office name. CDRH OCE Speaker Request webform collects the following non-PII information involving event details, some of which include event purpose, location, number of attendees, sponsoring organizations, and presentation details. PII is stored in accordance with the National Archives and Records Administration (NARA) records retention schedule.
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 Password
PTA 06:	Describe why each type of information is collected, maintained, and/or	The SalesForce Government Cloud environment

	shared by the system. Specify what information is collected about each category of individual.	provides both Platform as a Service (PaaS) and Software as a Service (SaaS) deployment models. The PaaS is comprised of the Force.com offering and SalesForce services are the SaaS offering. The current SalesForce Government Cloud infrastructure resides in two geographically separated data centers, acting as a primary facility and the other as a back-up "warm site." SalesForce manages the entire cloud infrastructure to include the data centers, network, data storage, system resources, and the platform and application software. Customers (FDA and its programs and offices) are responsible for configuring the platform and application capabilities and establishing any required customization through application development and application programming interface (API) integration. The salesforce Government Cloud provides a trusted and secure service to the U.S. Government, U.S. Government Contractors and Federally Funded Research and Development Center (FFRDC) customers in a quick and secure manner. The PaaS offering, available on the Force.com platform, provides a platform for the FDA to develop custom applications on-demand without the need of additional software via easy-to-use point and click tools. The SaaS offering is available via SalesForce services. These are SalesForce-built applications that are available to customers and can be implemented to meet various business needs. SalesForce is responsible for all service delivery layers to include: infrastructure (the hardware and software that comprise the Salesforce Government Cloud), data security and service management processes, i.e. the operation and management of the infrastructure and the system and software lifecycles. The overarching Salesforce platform and services addressed in this assessment do not entail the creation, collection, maintenance, processing, transmitting or other handling of PII or other data, including access credentials (username, password). Likewise, FDA does not use names or other identifiers to retrieve records from the assessed technology; it holds no data to retrieve. No PII is used to retrieve records from the Internal FDA Administrative Portal, FDA internal and external webforms. Accountable FDA/CDRH personnel designated as owners of applications they ultimately host or operate on this Salesforce technology are responsible for the PII and other data that is collected, stored, displayed and/or transmitted the applications they own. These application owners must ensure their data use and collection is compliant with all applicable laws, Executive Orders, regulations, and policies. PII data collected/stored in the Salesforce system (not platform): (a) first name and last name; (b) work email; (c) phone number; and (d) company

		address. FDA/CDRH personnel currently use PII to communicate with external contacts and organizations to provide help desk/inquiry management services. The Salesforce platform and application user community includes: FDA employees, Industry (Manufacturers: Citizens/Companies and Speakers: Citizens/Companies/Organizations/Non-Profits), and FDA Direct Contractors. The Internal FDA Administrative portal users include Administrators (FDA Direct Contractors) and Developers (FDA Direct Contractors) from various CDRH centers (OSEL, DICE, DHCoE and Payor). Users access the system is through SSO. Credentials are stored within Salesforce and users are required to be connected to the FDA network. Access to the internal webform hosted on the FDA network, via a link, is through the web browser, using a username (generated by Salesforce) and password (generated by the user). Credentials are stored within Salesforce and users are required to be connected to the FDA network, username and password is stored in Salesforce. All external webform users access the Webform, hosted on the FDA network, via a link (no credentials required). External users do not have access to the Salesforce platform.
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://fda-cdrh.my.salesforce-sites.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.	The purpose of the webforms is to collect information from external users in order for FDA to best assist them. FDA recently used the Salesforce platform to create an Internal FDA Administrative Portal, related webforms for internal and external users, and a COVID-19 portal, to enable collection of information, including PII, necessary for FDA work. The Salesforce applications in use include: Internal FDA Administrative portal, Internal FDA webform, and External FDA webforms. FDA internal webforms: CDRH Critical Path project users currently utilize the internal webform (for FDA employees and Direct Contractors) within Salesforce to manage the submission from internal employees in order to help gauge/handle and administrate ideas from FDA employees and process funding requests for said proposals. The Internal FDA Administrative portal users include Administrators (FDA Direct Contractors) and Developers (FDA Direct Contractors) from various CDRH centers (OSEL, DICE, DHCoE and Payor). Users access the system is through SSO. Access to the internal webform hosted on the FDA network, via a link, is through the web browser, using a username (generated by Salesforce) and password (generated by the user). All external webform users access the Webform, hosted on the FDA network, via a link (no credentials required). External users do not have access to the Salesforce platform. FDA external webforms- The webforms below provide external users (public citizens) the ability to submit inquiries to CDRH. All webforms are unauthenticated and do not share/expose any data with/to the external user and are accessible through via FDA.gov. Submitted forms are saved internally in Salesforce. Users with internal FDA Salesforce access and express permissions can access the internal side of Salesforce. Links are or will be available FDA.gov
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 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.	Identifying Numbers Device Identifiers DUNS Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	FDA Entity Identifier (FEI) number Potential combination of employment information data elements
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100,000 – 999,999
PIA 25:	For what primary purpose is the PII used?	The primary use of PII in Salesforce is for account registrations, contacting the individuals, case creation, and notification tracking.
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.	5 U.S.C. 301, The Food, Drug and Cosmetics Act, 21 U.S.C. 301
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 Email Online Non-Government Sources Members of the Public
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).	0910-0491 Expiration 10/31/2027 0910-0485 Expiration 07/31/2028

PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Submitters provide their contact information as a practical requirement in order to communicate with FDA and to gain access to the system. There are no opt-out procedures specific to Center for Devices and Radiological Health (CDRH) Salesforce. While FDA requires that regulated entities supply the PII of a point of contact, that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	No such changes are anticipated. If FDA changes its practices with regard to the collection or handling of PII related to the CDRH Salesforce system, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.
PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have many avenues available for assistance. Employees with such concerns can additionally work with their supervisors, the Privacy Office, a 24-hour technical assistance line, and FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). Contact information for these offices and resources is available across FDA's internet and intranet pages. All personnel are required to report suspected instances of PII compromise or misuse to 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.	Individuals voluntarily provide their PII. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. PII relevancy is supported through the design of the system to require and collect only the PII 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 (role-based access). Integrity and availability are protected by privacy and security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. CDRH performs annual reviews to evaluate user access.
PIA 38:	Identify who will have access to the PII in the system.	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.	Administrators: System administration Contractors: System administration Access is needed in order to administer the application and troubleshoot issues. Additionally, access is required to provide internal users with the ability to manage incoming inquires, manage contacts and leads, and manage device shortage notifications.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System administrators and Direct Contractors who are supporting the system and require access to PII, will submit an email request to their supervisor before access is given and approved.
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.	Access to the PII is based on user profile, role and privileges with level of access approved by system administration officials and enforced through technical settings and controls, as well as periodic reviews of user access.

PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that training has been successfully completed.
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).	Retention and destruction of PII is managed according to the authorized FDA and CDRH Records Retention Schedule and IT procedures. For the assets assessed in this PIA the records control "FDA-8122 Routine Correspondence (Program Office Correspondence)" is used. The National Archives and Records Administration (NARA) records retention schedule is N1-088-06-003, Item 1.2.2. The disposition is TEMPORARY. Media neutral. Cut off at end of each calendar year in which a response has been signed or correspondence received for which no response is needed. Destroy or delete 5 years after cutoff.
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 that PII entered via these systems is immediately pulled through the web-based systems into internal systems not connected to the web, removed from the public site, and not accessible to others submitting information via these systems or fda.gov. Physical controls include that all system servers are located at FDA 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. FedRAMP security procedures and controls are inherited from Salesforce. Additional best practices and procedures are in place to further restrict system/user access.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	8/11/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	8/11/2025
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:**	8/13/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 8/13/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	2

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	8/13/2025
SAOP Review Comments:	Approved on behalf of the SAOP	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
8/13/2025 8:33 AM	BLAND, CRYSTAL	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	8/12/2025	8/12/2025 Per FDA's Email: The attached PIA is SOP approved and should be in your queue. 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)?" o The FDA instance of Archer is automatically entering the answer "No," which is incorrect. The ATO date is 8/18/2023. o At this time, we are unable to update Archer to reflect the correct answer "Yes." The FDA Archer Team is aware of this occurrence and is working on a solution.	8-12-2025 EMAIL (CDRH SalesForce Applications) PTA _ PIA 4950091.pdf CDRH Salesforce Applications_SOP Approved.pdf