Privacy Impact Assessment (PIA): FDA - TRLM-NG - QTR4 - 2024 - FDA4323940

Created Date: 10/17/2024 8:25 AM Last Updated: 11/13/2024 12:31 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	FDA - TRLM-NG - QTR4 - 2024 - FDA4323940	**PIA ID:**	2328413
Name of Component:	FDA - CTP Tobacco Registration and Listing Module, Next Generation	**Name of ATO Boundary:**	CTP Tobacco Registration and Listing Module
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	27
Submission Status:	Submitted	**Submit Date:**	10/17/2024
Next Assessment Date:	N/A	**Expiration Date:**	11/13/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4323940
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	1/10/2023
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	There are no major changes to Tobacco Registration Listing Module Next Gen (TRLM NG). The PIA is now updated to reflect the new application point of contact (POC), and that the system is in operation.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	Tobacco Registration Listing Module Next Gen (TRLM NG) is hosted in the Food and Drug Administration (FDA) Amazon Web Services (AWS) Government Cloud Infrastructure as a Service (IaaS) based system designed to provide a seamless way for tobacco manufacturers to register their products to meet FDA regulatory standards. The purpose of TRLM NG is to allow tobacco manufacturers to register products in accordance with FDA policy. The system allows Center for Tobacco Products (CTP) to modernize current processes and systems and bring them into a cloud environment. In addition to supporting internal FDA processes, the platform streamlines business functions that require communication with personnel outside the FDA. Tobacco product manufacturers are required to register their products with the FDA twice per year to meet regulatory compliance standards. Internal FDA users can access the system to review the products, registrations, tobacco establishment addresses, certifications, and material files (product labels) uploaded to the application, approve establishments, products, and for establishment, product, and material file reporting. The Registration and Listing (R&L) site is included in the TRLM NG Authorization to Operate (ATO) boundary and evaluated in this assessment as well. The R&L site is also hosted on the AWS Government Cloud IaaS based system. Registration and listing information are provided and periodically updated by regulated entities. FDA has posted the information submitted to TRLM NG via R&L publicly as a means of providing public access to the information, which is required by Section 905(f) of the Tobacco Control Act, and as a service to interested stakeholders.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	TRLM NG is hosted in the FDA's AWS environment and is capable of hosting low or moderate sensitivity/impact tobacco product information and personally identifiable information (PII). FDA data resides in logically separated domains enabling the FDA to maintain complete control over all data stored. While tobacco product information in the system is publicly available, user PII remains confidential and unavailable for public view; however, product owner names (first and last) and operator names (first and last), both considered PII will be available for public view and search in the R&L site. Internal FDA CTP users access the application using PingFederate single sign-on (SSO). External users access the application using username and password, created by the user when registering for the application. PII collected and stored within TRLM NG from tobacco manufacturers includes name (first and last), email address, username and associated password, and phone number. This PII information

		is collected from the tobacco manufacturers as part of the registration process and in the event, they must be contacted. Non-PII in the form of tobacco manufacturer address is also collected. In addition, PII is also collected and stored from internal FDA CTP employees including name (first and last), email address, and phone number. This internal PII is collected for the purposes of basic user information. Tobacco product information, which is considered non-PII, that is collected and stored within the system includes: product name, product identification number, product identification number type (item catalog number, stock-keeping unit (SKU) number, UPC number), intended use of product (consumer use, further manufacturing use), product category, sub category (if "Other", user must specify), open/closed system, flavor, advertising, labeling, consumer information, and the date the product was introduced. This information is collected to aid the Center for Tobacco Products with carrying out the Family Smoking Prevention and Tobacco Control Act. PII and other data is stored in the FDA AWS Government Cloud environment. R&L includes the following data, provided by submissions to TRLM NG: establishment name, establishment state, FDA Establishment Identification (FEI) number, establishment operation type, operation type, operation address, owner name, product name, intent of use, product category, product name, product category; all which is considered non-PII. The PII included in R&L is the following: owner name (first and last) and operator name (first and last). The following data types are searchable on R&L: establishment name, establishment state, FEI number, owner name, establishment operation type, operator name, product name, intent of use, product category.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	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 - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	TRLM NG is an application built within the FDA's AWS Government Cloud IaaS environment and is designed to allow tobacco manufacturers to register products in accordance with FDA policy. Users of the system include internal FDA CTP users and tobacco manufacturers. PII collected and stored from CTP users include their name (first and last), email address, and phone number. Internal FDA CTP users will access the system through PingFederate SSO. External users will access TRLM NG to register their tobacco products with the FDA, using username and password to authenticate into the system. The PII collected and stored from tobacco manufacturers (external users) includes the following: name (first and last), email address, username and associated password, and phone number. Non PII data collected and stored within the system includes tobacco product name, product identification number, product identification number type (item catalog number, SKU number, UPC number), intended use of product (consumer use, further manufacturing use), product category, subcategory (if "Other", user must specify), open/closed system, flavor, advertising, labeling, consumer information, and the date the product was introduced. TRLM NG data is stored in the FDA AWS Government Cloud environment. Users (FDA employees and tobacco manufacturers) of the TRLM NG system retrieve system records using PII in the form of owner name (first and last), email address, operator name (first and last) and email address, point of contact (POC) name (first and last), email address, and phone number. Users use PII to retrieve records held in the system for the purpose of contacting the user or POC. The retrieved records contain the following information: name, establishment address, email address, phone number.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes

PTA - 9:	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 industry website is to allow tobacco manufacturers to register products in accordance with FDA policy. The internal website allows FDA users to access the system to review the products, registrations, tobacco establishment addresses, certifications, and material files (product labels) uploaded to the application, approve establishments, products, and for establishment, product, and material file reporting. The Registration and Listing (R&L) site provides public access to the registration information, which is required by Section 905(f) of the Tobacco Control Act.
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 - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
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 - Collect PII
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	

PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The primary purpose of PII in the TRLM NG system is to create, manage, and communicate regarding registrations, listings, and associated industry users registering products through TRLM NG. Username and password are used to ensure controlled, secure access to the system. Email and mailing address are used to communicate with industry users regarding any action taken on submissions including new account creation, deactivation, temporary passwords for password reset, new submissions, status changes, and other actions. PII, including owner name and operator name (both first and last names) are viewable and searchable on R&L to find associated tobacco product and establishment information.
PIA - 5:	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 - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	FDA issues export certificates under Section 801(e) or 802 under the Export Reform and Enhancement Act of 1996. Sections 510 and 905 of the Food, Drug, and Cosmetic Act (FD&C, codified at 21 U.S.C. 360 and 387e) require establishments (e.g., manufacturers, re-packers, and re-labelers) to register with FDA upon engaging in the manufacture, preparation, propagation, compounding, or processing of FDA regulated products, including tobacco. Statutory citations: 21 U.S.C. 331, 374, 381, 387e, 393, 5 U.S.C. 301.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Owner Name and Operator Name.
PIA - 8B:	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: 09-10-0002 Regulated Industry Employee enforcement Records, HHS/FDA/OC

PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB control number 0910-0650
PIA - 10B:	Identify the OMB information collection approval number expiration date.	10/31/2025
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	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.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	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 TRLM NG. 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 - 14:	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). Alternatively, describe why they cannot be notified or have their consent obtained.	No such changes are anticipated. If FDA changes its practices with regard to the collection or handling of PII related to the TRLM NG 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 email to individuals, adding or updating online notices or forms, or other available means to inform the individual. In addition, HHS/FDA would publish a revised System of Records Notice (SORN) in the Federal Register and update the PIA.

PIA - 15:	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 options available for assistance. These individuals may contact FDA offices, including the CTP TRLM NG program manager, the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov and the FDA intranet).
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. 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 authorization to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. CTP performs annual reviews to evaluate user access.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: FDA employees and tobacco manufacturers will have access to their own PII in the system and can edit it for changes. Administrators: Will have access to user PII when needed for TRLM NG administrative tasks. The development team will have administrator accounts in pre-production environments. Developers: Will have access to user PII for system development, implementation, and operations and maintenance tasks

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and tobacco manufacturers with valid network accounts who require access to TRLM NG must obtain supervisory approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	The relevant supervisor indicates on the TRLM NG user account creation form the minimum access that is required in order for the user to complete his/her job. The scope of access is restricted based on role-based criteria.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system 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).
PIA - 22:	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 - 23:	Describe the process and guidelines in place with regard to 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 agency continuously reviews the retention and destruction process associated with the information contained within TRLM NG to ensure it complies with FDA and NARA regulations. Applicable records control schedule: FDA file code 7210 and 7222 for Registration and Listing files and system database records; NARA approved citation N1-88-07-2. Disposition: Temporary – Cutoff after establishment goes out of business or product is not commercially marketed. The certificate modules delete/destroy after 5 years. All other modules delete/destroy 10 years after cutoff or when no longer needed for legal, research, historical or reference purposes, whichever is the latest. If data was migrated into a new system or replaced by a successor system, delete/destroy it after the verification of successful data migration. From the LACF PIA: FDA file codes 7330-7225 (NARA approved citation nos. N1-88-07-2 and General Records Schedule 20-2a, 2b, 4-7, 12, 16) cover FDA's Registration and Listing Systems. These files are temporary and are destroyed when no longer needed, the establishment goes out of business, the product is no longer marketed, destroyed 10 years after cutoff.

PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the NIST's Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	10/17/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP 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.	**SOP Review Date:**	10/17/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/21/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 10/21/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	4

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	11/13/2024
		SAOP Days Open:	23

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CTP Tobacco Registration and Listing Module_SOP Approved.pdf	177389	.pdf	10/17/2024 8:40 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	VILLAFUERTE, NESTOR	10/17/2024	Per the PTA, please add user credentials as one of the PII elements collected.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	11/13/2024 12:31 PM	**History Log:**	View History Log