Privacy Impact Assessment (PIA): FDA - END - QTR1 - 2025 - FDA4901490

Created Date: 2/18/2025 11:28 AM Last Updated: 3/3/2025 4:04 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 - END - QTR1 - 2025 - FDA4901490	**PIA ID:**	2784364
Name of Component:	FDA - OC Enterprise Network Devices	**Name of ATO Boundary:**	OC GSS1 Network and Telecom
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	24
Submission Status:	Submitted	**Submit Date:**	2/12/2025
Next Assessment Date:	N/A	**Expiration Date:**	3/2/2028
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4901490
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)?	No
4:	ATO Date or Planned ATO Date.	9/7/2022
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.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
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.	The Food and Drug Administration (FDA) organizes its information technology infrastructure into five General Support Systems (GSS). Each of these GSS focuses on a specific theme within the Information Technology (IT) portfolio at the FDA. GSS 1 is one of these five General Support Systems that comprise the FDA's consolidated infrastructure, known as the Office of the Commissioner (OC) Consolidated Infrastructure (OC CI) system. The subject of this assessment is the Enterprise Network Devices (END) component/subsystem of GSS1. Other GSS 1 components are assessed separately. The FDA OC CI END system is comprised of network and security devices that are typically configured and operate independently, outside of consistent human interaction. For example: routers, switches, load balancers, Domain Name System (DNS) appliances, Virtual Private Network (VPN) appliances and other IT devices. The END is managed by the FDA Office of Information Management and Technology (OIMT) Infrastructure and Engineering Branch and provides the boundary protection for the FDA network. The purpose of Enterprise Network Devices is to provide secure network connectivity between FDA users located across the United States. The END also provides network connectively to internal application servers and the Internet to FDA users. Additionally, END provides access to select public facing applications for the general public.
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.	The END system holds system-specific access credentials such as usernames and passwords. Usernames are provided by a system administrator, and the passwords are provided by the user. END also collects the following Personally Identifiable Information (PII): first and last name, professional or personal email address (depending on the user), and personal or professional phone number.
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.	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.	The END system holds system-specific access credentials such as usernames and passwords. Usernames are provided by a system administrator, and the passwords are provided by the user. END also collects the following Personally Identifiable Information (PII): first and last name, professional or personal email address (depending on the user), and personal or professional phone number. This PII is collected to manage access control and ensure that the correct users have access to the system.

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?	No
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
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.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
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?	
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	
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.	Business Partners/Contacts (Federal, state, local agencies) 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 the PII data collected in END is so that access control can be monitored and granted for auditing purposes.
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.	5 U.S.C. 301
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
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.	
PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	This does not fall under the definition of "information collection request" in the Paperwork Reduction Act.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	PII is shared with HHS for identification and access management purposes. It is shared with HHS Security Operations.
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)).	A Memorandum of Understanding (MOU) exists between FDA and HHS for the sharing of PII.

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.	N/A. PII is not shared outside HHS and thus no accounting for disclosures is required.
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.	An individual may opt out of providing their PII to the FDA. Should an individual choose to do this, they will not be able to perform their job duties at the FDA. The external individual that is visiting the FDA may decline to provide the required PII for guest wireless internet access. However, if they choose not to provide their PII data, they will not be able to access or login to the FDA Guest Wireless network.
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 major changes are planned or anticipated. If FDA changes its practices with regard to the collection or handling of PII for END, FDA 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 - 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.	The individual may contact their FDA sponsor and inform them of their request to have their guest wireless internet access revoked and have their PII removed from END. FDA employees may contact a system administrator or the Employee Resource and Information Center (ERIC). 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). External individuals may contact the FDA Privacy Office, their FDA point of contact or general points of informational contact at the FDA. 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 - 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.	PII is provided voluntarily by the individual. 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. Relevancy is supported by design of system and related processes to solicit or collect only the PII necessary for the system's purpose and supporting functionality. 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 NIST guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. FDA's Office of Information Management and Technology (OIMT) performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified in the course of system use are addressed when discovered.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Administrators: System operation monitoring and troubleshooting purposes. Some of the Administrators are Direct Contractors. Contractors: For system operation monitoring and troubleshooting purposes. Some of the Administrators are Direct Contractors.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA Form 3530 is signed by an appropriate supervisor and the system owner, which determines who will have administrative access to the system. Upon approval by the appropriate supervisor, users are assigned role-based access which applies the concept of least privilege and need-to-know enforced.

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.	Only the minimal amount of PII data is collected by the system. It is a common practice of the FDA to collect system or application specific access credentials in order to manage accounts and ensure users can access the system / application securely. The system also employs Role-Based Access Control (RBAC) which ensures users have the minimum level of access required to complete day-to-day job duties.
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 awareness training (CSAT). 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 - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All system administrators must complete additional rules of behavior training, and role-based training.
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 records in END are maintained under the following National Archives and Records Administration (NARA) citation; General Records Schedule (GRS) 3.1 item 20. The disposition of these records is temporary, and they are destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is deemed obsolete, completed, terminated or superseded. A longer retention is authorized if required for official business use. WLAN does not contain PII.

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 National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. The Rules of Behavior for using FDA systems are clarified and mandated to the user by the HHS guidelines and security documentation. Users agree to abide by these rules when receiving access to FDA systems and upon passing a background clearance check.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	2/18/2025
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:**	2/18/2025
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/19/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 2/19/2025 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	The PIA is experiencing an Archer error with Question #3 of the general information. • Q-3 "Does the system have or is it covered by a Security Authorization to Operate (ATO)?" • The FDA instance of Archer is automatically entering the answer "*No*," which is incorrect. The ATO date is 9/7/2022. • 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.	**SAOP Review Date:**	3/3/2025
		SAOP Days Open:	12

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
2-18-2025 EMAIL_PIA in Queue (OC Enterprise Network Device).pdf	395099	.pdf	2/18/2025 12:49 PM	0
OC Enterprise Network Devices_SOP Approved.pdf	160877	.pdf	2/18/2025 12:49 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	2/19/2025	Archer issue impacting the PIA: The PIA is experiencing an Archer error with Question #3 of the general information. • Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” • The FDA instance of Archer is automatically entering the answer “*No*,” which is incorrect. The ATO date is 9/7/2022. • 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.	
PIA - 23	VILLAFUERTE, NESTOR	2/19/2025	Please define WLAN on its first instance.	

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:	3/3/2025 4:04 PM	**History Log:**	View History Log