PTA / PIA: FDA - NAC - QTR3 - 2025 - FDA4948800

Created Date: 7/2/2025 12:21 PM Last Updated: 7/2/2025 4:23 PM

General Information

PTA / PIA Name:	FDA - NAC - QTR3 - 2025 - FDA4948800	**PTA / PIA ID:**	3442482
Component Name:	FDA - OC Network Access Control	**ATO Boundary Name:**	OC GSS1 Network and Telecom
Overall Status:	Complete	**# of Days - Open:**	1
Submitter:		**Submit Date:**	7/2/2025
Next Assessment Date:	07/01/2028	**Expiration Date:**	7/1/2028
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.	9/27/2022
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: Tiffany Coleman
PTA 01A:	POC Title and Organization	POC Title: IT Specialist POC Organization: FDA
PTA 01B:	POC Email Address	tiffany.coleman@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-5140
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.	Since this Privacy Threshold Analysis/Privacy Impact Assessment was last approved, FDA made changes to include refreshing hardware devices and removing end of life (EOL) hardware devices; removed access guest wireless fidelity (Wi-Fi); and updated the operating system (OS) on management servers.
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) 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 overarching consolidated infrastructure, known as the Office of the Commissioner (OC) Consolidated Infrastructure (OC CI) system. Within OC CI, FDA's Network Access Control (NAC) system falls under GSS 1 which provides network resources, equipment, hardware, and software utilized by the FDA and its users. FDA NAC is part of the FDA's defense in depth architecture strategy. This architecture is designed to enhance the security posture of the FDA's networks. The FDA's implementation of NAC ensures that only authorized devices such as desktops, laptops, tablets, or mobile phones can gain access to the FDA's regulatory and scientific networks. FDA NAC also provides guest internet access capabilities to authorized FDA visitors who use the FDA wireless local area network (WLAN) for conducting official FDA business. FDA guests will be provisioned for "Internet only" access when they request such access from an FDA full time equivalent (FTE) also referred to as a sponsor. This guest access is authorized only for the duration of the guest's visit to an FDA building or site.
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.	NAC collects the following Personally Identifiable Information (PII): (a) first and last name; (b) work e-mail address; (c) phone number; and (d) FDA issued device certificates/identifiers. The collected PII can either be personal or professional contact information. The PII for authorized visitors and FDA employees is retained for a period of fifteen days after the conclusion of the Guest Internet Access request. The PII in this system is not shared with any other system or organization.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Active Directory

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.	FDA NAC is part of the FDA's defense in depth architecture designed to enhance the security posture of the FDA's networks by ensuring that FDA authorizes devices such as desktops, laptops, tablets, or mobile phones that request access to the FDA's regulatory and scientific networks. FDA NAC also provides Guest Internet access capability via a Verizon Internet Service Provider (ISP) circuit, to authorized FDA visitors using FDA wireless local area network (WLAN, within FDA's United States facilities) for conducting official FDA related business. FDA guests are provided "Internet only" access when they request such access from an FDA full time equivalent (FTE) also referred to as a guest sponsor. This guest access is limited in time to the duration (1 to 90 days per request) of the guest visit and provided only for business requirements. FDA employees and Direct Contractors are not allowed to use the Guest Internet Access for their daily work or personal use. They are required to use the FDA wireless fidelity (FDA-WiFi) and/or the FDA wired network for their daily work or limited personal use. FDA Office of Information Technology (OIMT) personnel assigned as system administrators and/or operators use PII to retrieve Guest Internet Access request records including using the guest's first name, last name, email address, and/or telephone number of FDA sponsored guests.
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://wodc-esnisepan-01.fda.gov/ https://adc-esnisepan-01.fda.gov/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No

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 Cisco Identity Services Engine (ISE) web interface is used internally by FDA IT and network security personnel to manage and monitor Network Access Control (NAC) policies. Its primary purpose is to enforce access control rules based on user identity, device posture, and network location, ensuring that only authorized and compliant users and devices can access FDA network resources. Access to the Cisco ISE interface is strictly limited to a designated group of FDA personnel, including network administrators, cybersecurity team members, and approved system engineers, all of whom are required to have the appropriate clearance and role-based permissions. The interface is not publicly accessible and can only be reached through the FDA's internal network or via a secure virtual private network (VPN) connection. Users access the web interface through a secure hypertext transfer protocol secure (HTTPS) connection and must authenticate using multi-factor authentication (MFA). All access and administrative activity is logged and monitored in accordance with FDA's security and auditing policies.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Device Identifiers Biographical Information Name Contact Information Email Address (Personal) Phone Numbers (Personal) Email 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.	FDA issued device certificates/identifiers. NAC is for any category of individual who may visit an FDA building or site and require access to an internet connection.
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 Grantees Patients Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	10,000 – 49,999
PIA 25:	For what primary purpose is the PII used?	The primary purpose of the PII data that is collected by NAC is to provide guest internet access capabilities to authorized FDA visitors who use the FDA’s WLAN for conducting official FDA business while visiting an FDA campus in the United States.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The FDA makes no secondary use of the PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The legal authorities that govern information use and disclosures specific to the system and program are: 5 U.S.C. 301 and the Privacy Act.
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.	The PII data elements that are used to retrieve records in the system/system component/information collection are: Username (e.g., Active Directory or Lightweight Directory Access Protocol (LDAP) account), Media Access Control (MAC) address (can be tied to a specific user/device), Internet Protocol (IP) address, E-mail address, Hostnames, Certificate Subject Distinguished Name (DN) / Common Name.
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.	OPM/GOVT-1 General Personnel Records, OPM 09-90-0777 Facility and Resource Access Control Records
PIA 30:	Identify the sources of PII in the system.	Government Sources Other HHS OPDIV Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet Private Sector

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 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?	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.	The person that is visiting 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 Internet Access network.
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 major changes are planned or anticipated. If FDA changes its practices with regard to the collection or handling of PII for NAC, 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.	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 NAC. 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 FDA personnel can report suspected misuse or unauthorized disclosure of their PII through: Designated Privacy Officer or the Cybersecurity and Infrastructure Operations Coordination Center (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.	The information retained in NAC is temporary and automatically removed by the system within one to fifteen days from the expiration date of the guest's wireless internet access account. A visitor's PII is provided voluntarily by the individual. The individual is responsible for providing accurate information. Accuracy is ensured by the individual at the time of providing the PII to the authorized sponsor. 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 and duration on the FDA campus (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.

The process in place for periodic reviews of PII to ensure the data integrity is:

Cisco ISE is integrated into the organization's broader IT governance framework. To ensure the integrity of PII, the system undergoes regular reviews that include:

Automated validation of identity attributes via synchronization with authoritative sources (e.g., Active Directory or Lightweight Directory Access Protocol (LDAP)) to detect inconsistencies or unauthorized changes.

Audit logs and integrity monitoring tools (e.g., file integrity monitoring, configuration checks) to detect tampering or unauthorized modification of PII.

Quarterly data validation checks by the Security Office to confirm data integrity.

Use of cryptographic protections (Transport Layer Security (TLS), certificates) to maintain data integrity in transit and at rest.

The process in place for periodic reviews of PII to ensure data availability is:

To maintain the availability of PII data in Cisco Identity Services Engine (ISE):

Redundancy and failover configurations are implemented (e.g., distributed deployment with primary and secondary policy nodes).

Backup and disaster recovery plans are in place, with scheduled backups (daily or weekly) and offsite storage.

Annual testing of recovery procedures ensures the data can be restored with minimal downtime.

System uptime and performance monitoring (via SNMP (Simple Network Management Protocol), system logs (syslogs), and dashboards) helps proactively identify and correct issues impacting data availability.

The process in place for periodic reviews of PII to ensure data relevancy is:

To ensure data relevancy, the organization:

Conducts biannual reviews of user accounts,

		endpoint records, and identity profiles to determine if the information remains current and necessary. Accuracy of PII is ensured: The accuracy of PII in Cisco ISE is maintained through: Automated synchronization with authoritative identity sources, such as Active Directory or HR systems, ensuring updates are reflected in near real-time. Periodic manual audits conducted by designated personnel to verify that stored identity attributes match current records. Access control policies that prevent unauthorized edits to PII, limiting changes to trusted system administrators or through approved workflows.
PIA 38:	Identify who will have access to the PII in the system.	Administrators Contractors Others
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 38C:	Identify the additional person(s) who will have access to the PII in the system not mentioned in the list above.	Sponsors have access to the information that they have entered into the system for their guests. Sponsors are granted this access to facilitate changes to Guest Internet Access modifications to the original request.
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Administrators: System administrators to operate and maintain the system. Some of the administrators are Direct Contractors. Contractors: Some system administrators who are Direct Contractors require access to operate and maintain the system. Other: Sponsors have access to the information that they have entered into the system for their guests. Sponsors are granted this access to facilitate changes to Guest Internet Access modifications to the original request.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	There are two user groups who can access PII: (a) System Administrators, and (b) Sponsors. Administrators require access to PII in order to operate and maintain the system which allows access to all system resources. Sponsors are required access to PII of their guest in order to validate their guests who are requesting access within FDA facilities. The administrative procedures in place to determine which system users may access PII are: Access to Personally Identifiable Information (PII) within the Cisco ISE system is strictly controlled and governed by established administrative procedures designed to uphold the principles of least privilege, need-to-know, and role-based access control (RBAC). These procedures ensure that only authorized personnel—such as administrators and contractors—are granted access to PII, and only to the extent necessary to perform their official duties.
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.	The following technical methods are in place to allow those with access to PII to only access the minimum amount of information necessary to perform the job: Cisco ISE integrates with enterprise identity and access management systems and employs multiple layers of technical controls to ensure users only access the minimum necessary PII required for their role. Using Role-Based Access Control (RBAC), Users are assigned to specific roles, and each role is configured to allow access only to the functions and data types necessary based on job function. RBAC ensures that PII (like usernames, IP address associations, endpoint details) is not visible to unauthorized roles.
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 users are required to complete the following training and awareness programs to make them aware of protecting PII: Privacy Awareness Training and Cybersecurity Annual Training. The Office of Digital Transformation (ODT) tracks completion of the course.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users. However, users are provided with user guides and manuals, and privacy guidance is available on the FDA intranet.

PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The following process and guidelines are in place for the retention and destruction of PII: Regular data audits and reviews are conducted to identify PII that has reached the end of its retention period. The specific National Archives and Records Administration (NARA) records schedule is General Records Schedule (GRS) 3.2 Item 030, System Access Records. Disposition: Temporary. Destroy when business use ceases.
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 secures PII in the system using the following administrative controls: Policies and Procedures: Comprehensive privacy and data protection policies govern the collection, use, retention, and disposal of PII. Access Management: Formalized user access request, approval, and periodic review processes ensure only authorized personnel have access to PII. Training and Awareness: Mandatory annual privacy and security training for all users handling PII, emphasizing FDA's data protection responsibilities. Incident Response: Established procedures for reporting, investigating, and responding to potential privacy breaches or unauthorized disclosures. Contractor and Third-Party Oversight: Privacy requirements are incorporated into contracts, and regular assessments to ensure compliance. Role-Based Access Controls (RBAC): Defined roles and responsibilities restrict PII access to users based on job function and necessity. FDA secures PII in the system using the following technical controls: Encryption: PII is encrypted both in transit (e.g., transport layer security (TLS) 1.2+) and at rest using federal information processing standards (FIPS) 140-2 validated cryptographic modules. Access Controls: Implementation of RBAC and least privilege principles within the system, enforced through authentication and authorization mechanisms. Multi-Factor Authentication (MFA): Required for privileged accounts and remote access to systems containing PII. Audit Logging and Monitoring: Continuous logging of access and changes to PII, with automated alerts for suspicious activities. Data Masking and Redaction: Sensitive PII fields are masked or redacted based on user roles to

limit exposure.

Vulnerability Management: Regular scanning, patching, and security updates reduce risks of exploitation.

Network Security: Firewalls, intrusion detection/prevention systems (IDS/IPS), and segmentation protect systems containing PII.

FDA secures PII in the system using the following physical controls:

Secure Facilities: Data centers and offices housing FDA systems are protected by controlled physical access including badges, biometrics, and security guards.

Equipment Security: Computers and servers containing PII are secured in locked rooms.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	7/2/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	7/2/2025
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:**	7/2/2025
Agency Privacy Analyst Review Comments:	7/2/2025 This PIA is ready for SAOP review.	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/2/2025
SAOP Review Comments:	Approved on behalf of the SAOP.	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/2/2025 1:40 PM	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	7/2/2025	7/2/2025 Per FDA's Email, 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 9/27/2022. 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.	7-2-2025 EMAIL_PIA in Queue (OC Network Access Control).pdf OC Network Access Control_SOP Approved.pdf