PTA / PIA: FDA - IDAM - QTR2 - 2025 - FDA4933473

Created Date: 6/5/2025 4:25 PM Last Updated: 6/24/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - IDAM - QTR2 - 2025 - FDA4933473	**PTA / PIA ID:**	3273844
Component Name:	FDA - OC Identity and Access Management	**ATO Boundary Name:**	OC GSS4 Enterprise Tools and Services
Overall Status:	Complete	**# of Days - Open:**	19
Submitter:		**Submit Date:**	6/10/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**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)?	Yes
General 04:	ATO Date or Planned ATO Date.	10/12/2022
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: Jake Yoder
PTA 01A:	POC Title and Organization	POC Title: SUPV IT SPECIALIST (INFOSEC) POC Organization: ODT/OIS
PTA 01B:	POC Email Address	Jake.Yoder@fda.hhs.gov
PTA 01C:	POC Phone Number	Phone: 202-868-7982
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, Food and Drug Administration (FDA) made the following changes to the Office of the Commissioner (OC) Identity and Access Management (IDAM): * Added NokNok, a new Phishing resistant MFA tool. * PingDirectory module was activated on to the existing PingFederate toolset.
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's (FDA) Office of the Commissioner Consolidated Infrastructure (OC-CI) consists of a number of General Support Systems (GSS1 – GSS5). Each GSS in turn consists of a number of tools, applications and components. This assessment addresses a subset of the components of FDA's GSS4, OC Identity and Access Management (IDAM) Component: Enterprise SailPoint Identity Governance and Administration (IGA), PingFederate (Ping), PingDirectory, PingAccess, Public Key Infrastructure (PKI), NokNok, and RadiantLogic. The Enterprise SailPoint Identity Governance and Administration (IGA) application is used for overall Identity and Access Management (IDAM) purposes including but not limited to provisioning/de-provisioning of user access to application entitlements via Active Directory Groups, customer defined Separation of Duties (SOD) policies, user access certification and reporting. Currently, there is a Lightweight Directory Access Protocol (LDAP) filter which only allots for the aggregation of the Center for Biologics and Evaluation and Research (CBER) users, and the initial deployment is for CBER Applications. Additional applications for different organizations will be onboarded in the future. SailPoint is accessed via federated Enterprise Identity and Authentication (EIA, also known as Active Directory (AD)) credentials facilitated by PING Federate using a Single Sign-On (SSO) process with multi-factor authentication). EIA (AD) is covered and assessed in a separate PIA. This process enables FDA to identify and authenticate individual users (FDA personnel, including employees and Direct Contractors) of agency IT resources as to ensure that each individual is who he/she purports to be, is properly associated with the agency computer assigned to the user, and has appropriately limited access to agency IT systems and to any defined user groups. PingFederate (Ping) is an enterprise federation server for user authentication and standards-based single sign-on (SSO) for employee, partner and customer identity types. PingFederate allows the FDA to leverage a modern identity and access management solution designed to meet complex

enterprise demands such as password-free authentication, life-cycle management, and multi-factor authentications. Ping utilizes current protocols to securely protect access to the FDA on-premises and cloud resources. Ping will validate identities via AD and Public Key Infrastructure (PKI) for personal identity verification (PIV) card-based authentication.

The FDA uses PKI to procure certificates for workstations and allow automatic connections to the Enterprise WIFI; procure certificates for domain controllers to enable PIV logins to occur; procure certificates for services/web applications to support trusted communications (i.e., HTTPS); and validate PIV/ALT-PIV and internally issued certificates.

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.	Enterprise SailPoint IGA: SailPoint will aggregate data from two data and identity sources. Active Directory attributes will be ingested as well as human resources data obtained from FDA's Enterprise Administrative Support Environment (EASE) system. SailPoint will then build Identity Cubes and correlate the data for each user. The HHS-Identification code is used for this correlation. There is also a manager attribute used for the manager correlation setting within SailPoint. There are scheduled automated tasks configured for both data sources which run daily to ensure user attribute information is up to date as well as the creation of new Identity Cubes and the deletion of Identity Cubes for users who are no longer here. SailPoint IGA collects the following personally identifiable information (PII) about users: (a) Name; (b) work email address (c) work mailing address; (d) work phone number; (e) employee ID; (f) employee number; (g) HHS identification code; (h) objectSid (unique numeric identifier associated with user accounts); and (i) sAMAccount name (system administrator account identifier). Users of SailPoint IGA consist of only CBER employees at this current time, which include FDA employees and Direct Contractors. User's access SailPoint IGA through SSO via Ping. Users of Ping consist of FDA employees and Direct Contractors. PingFederate is an enterprise federation server for user authentication and standards-based single sign-on (SSO) for employee, partner and customer identity types. PKI is internally facing. Certificates are typically automatically obtained via the Windows OS auto-enrollment facility. Computers will automatically reach out to the Certificate Authorities to request a certificate. The Certificate Authority then issues a certificate which is automatically installed. In the case of Services (i.e., FDA websites), the requester will connect to a Certificate Lifecycle Management System (aka CLMS) to request a certificate. The requester will supply his/her name and FDA email address, as well as a secondary email contact (i.e., manager or a team distribution list). The email addresses allow the CLMS to email the certificates, as well as expiration notifications. There are no user passwords used or saved. Users of PKI consist of FDA employees and Direct Contractors. Users access PKI through SSO. When an employee departs or is terminated, their information is deleted as per controls applied to the EASE and Active Directory systems, which are sources of record for this system.
PTA 05A:	Are user credentials used to access the system?	Yes

PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Email Address HHS Username
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The components assessed in this PIA collectively receive and maintain work contact and system user account information about users consisting of (a) Name; (b) work email address (c) work mailing address; (d) work phone number; (e) employee ID; (f) employee number; (g) HHS identification code; (h) objectSid; and (i) sAMAccount name. None of this PII is shared outside the FDA and internal sharing between FDA systems is limited to the PII that is necessary to achieve the purpose and function of the components – identity authentication and access management. Additionally, PII is not leveraged by users of the system to retrieve employee records. Although this information is searchable by sysadmins, not all PII attributes are searchable. For instance, items (e) through (f) are built into Active Directory which can uniquely identify a user but are not searchable. FDA personnel and Direct Contractors do not use PII to retrieve system records about individuals.
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://pki-cms.fda.gov/KeyfactorPortal https://ssoext.fda.gov https://sso.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 purpose of the website is to request PKI certificates. Only internal FDA users have access to the website. Users access the website via its Kerberos SSO.
PTA 10:	Does the website have a posted privacy notice?	No
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 Employee ID Number Biographical Information Name Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	employee ID, employee number, HHS identification code, objectSid (unique numeric identifier associated with user accounts), and sAMAccount name (system administrator account identifier)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	To uniquely identify all FDA application users accessing resources, authenticate their identities and to accurately transmit certificates and certificate expirations.
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
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.	Government Sources Within the OPDIV
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.	OC Identity and Access Management does not collect information from any persons other than federal employees/direct contractors, therefore does not require an OMB information collection approval number.
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.	Users 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 the system. Users who decide not to provide their PII to source systems would be unable to access the systems.
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.	If FDA changes its practices regarding the collection or handling of PII related to the website, 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. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity 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). In the event of a suspected incident or data breach, FDA personnel must report that without delay to the FDA's CIOCC.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	Individuals voluntarily provide their PII to the FDA and the source systems associated with components assessed in this PIA. 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 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 also performs annual reviews to evaluate user access.

PIA 38:	Identify who will have access to the PII in the system.	Administrators Developers 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.	The reason the administrators, developers, and contractors (HHS Direct Contractors) need access to PII is to maintain and administer the system.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system 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 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 relevant supervisor will indicate on the user account creation form the minimum access that is required for the user to complete his/her job. The scope of access is restricted based on role-based criteria.
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 Digital Transformation (ODT) verifies that individuals successfully complete the training.
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 acknowledge 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).	The system is maintained under NARA General Records Schedule (GRS) 3.2, Item 30, System Access Records. Disposition: TEMPORARY. Destroy when business use ceases. When an employee departs or is terminated, their record is deleted as per controls applied to the EASE and Active Directory systems, which are sources of record for this system. All systems go through quarterly user access review to clean up.

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 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.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/10/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/11/2025
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:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/12/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/12/2025 Comment was addressed all websites are only internal FDA users have access to the website. This PIA is ready for SAOP review and approval. 6/10/2025 Please see comment an update accordingly. PTA-08B: Per PTA-09, these websites are internal to FDA thus the URLs are not accessible to the public. The response to PTA-08B should be "No."	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	12

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/24/2025 3:32 PM	GUENTHER, BRIDGET	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	6/6/2025	Per FDA's Email included an attached copy of the PIA.	OC Identity and Access Management_SOP Approved_6.5.2025.pdf
PTA 08B	VILLAFUERTE, NESTOR	6/9/2025	Reviewer notes that none of the URL stated in the previous question were reachable, are these all internal websites? If so, please select "No".	