PTA / PIA: FDA - CDER Splunk - QTR2 - 2025 - FDA4941448

Created Date: 7/16/2025 9:08 AM Last Updated: 7/16/2025 12:39 PM

General Information

PTA / PIA Name:	FDA - CDER Splunk - QTR2 - 2025 - FDA4941448	**PTA / PIA ID:**	3498916
Component Name:	FDA - CDER Splunk Cloud	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	33
Submitter:		**Submit Date:**	6/13/2025
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.	5/22/2025
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Chao-Hui Sara Wu
PTA 01A:	POC Title and Organization	Title: Supervisory Operations Research Analyst POC Organization: FDA CDER/OSP/OBI
PTA 01B:	POC Email Address	Chao-hui.wu@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-6115
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	FDA has made no changes to this component since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Food and Drug Administration (FDA) Center for Drug Evaluation and Research (CDER) Splunk Cloud (SC) is a system that uses a vendor managed cloud solution called Splunk, which is a Software-as-a-Service (SaaS), hybrid cloud application. Splunk is a log aggregation and analytics tool to help aide FDA with monitoring and troubleshooting of their on-premises and cloud applications and infrastructure. This tool enables the CDER Office of Business Informatics (OBI) teams to ensure high data availability and quick issue resolution. It thereby supports CDER work overseeing the review and approval of human drug products to ensure that they are safe, effective, meet established quality standards, and are available to patients according for their intended use. Users of the CDER SC system consist of FDA employees and Direct Contractors. The internal CDER users' access CDER Splunk Cloud through FDA/CDER Single-Sign On (SSO) or the username/password option for monitoring, reviewing logs, performance and performing system troubleshooting.
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.	CDER SC collects the following personally identifiable information (PII) from users (FDA employees and Direct Contractors): (a) first and last name; (b) professional/work e-mail address; (c) work phone number and (d) username/password. This PII is obtained from FDA/CDER server logs and FDA retains the PII for three years. CDER Splunk Cloud does not have or maintain any external users. Information is stored in accordance with the National Archives and Records Administration (NARA) retention schedule.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Username Password

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.	CDER SC employs the Splunk Cloud SaaS, a cloud application to enable real-time log aggregation and system monitoring. There is no name or other PII is used to retrieve records. This tool enables the CDER OBI teams to monitor the system health and alerts in real time to ensure high system and data availability and quick resolution of issues impacting CDER informatics systems. CDER Splunk Cloud system will be used for log aggregation and monitoring in CDER Production environment only. PII collected about FDA personnel and Direct Contractors is obtained from FDA's Active Directory system, which is covered in a separate PIA. There are three user account types assigned to internal users of the system based on their role. Administrator accounts (super user) come with the most assigned capabilities to enable Administrators to manage users, objects, and configuration. "Power User" accounts enable each moderately-elevated user to create and edit his/her/their saved searches, run searches, edit preferences, create and edit event types, and execute other similar tasks. Standard user accounts provide the user the ability to create and edit his/her own saved searches, run searches, edit preferences, create and edit event types, and perform other similar tasks.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://fda-cder.splunkcloudgc.com/
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.	CDER Splunk is a log aggregation and analytics tool to help aide FDA with monitoring and troubleshooting of their on-premises and cloud applications and infrastructure. This tool enables the CDER Office of Business Informatics (OBI) teams to ensure high data availability and quick issue resolution. It thereby supports CDER work overseeing the review and approval of human drug products to ensure that they are safe, effective, meet established quality standards, and are available to patients according for their intended use. Access to this website is restricted to authorized Food and Drug Administration (FDA) employees and approved Direct Contractors who have successfully completed Single Sign-On (SSO) authentication with credentials maintained in the Active Directory. FDA Employees and authorized Direct Contractors login using SSO to access the system but also have the option to login using username/password.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Does Not Collect PII
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.	Biographical Information Name User Credentials Contact Information Email Address (Business) Phone Numbers (Business)
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.	<100
PIA 25:	For what primary purpose is the PII used?	The PII is collected for account management and authentication purposes and to troubleshoot and to perform system monitoring.

PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	Not applicable (N/A). No secondary uses for PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Provisions of the Federal Food, Drug & Cosmetic Act at 21 U.S.C. 301 including sections 353,355,356b, 360.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online 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.	This system/component 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.	There are no formal notice and consent procedures specific to this system. All users are internal. Individuals provide their contact information as a practical requirement of employment. Users are provided notice at the time of hire and consent to the agency's use and creation of PII about them as needed to administer FDA resources and activities. Each time personnel log on to the agency network they also view and acknowledge a notice and warning of the lack of privacy in the course of using FDA equipment and resources. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet pages. This PIA provides additional notice.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	No such changes are anticipated. If the FDA or CDER changes its practices regarding the collection or handling of PII related to the CDER Splunk Cloud system, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.

PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	There is no process in place specific to CDER Splunk Cloud. Individuals may contact the FDA CDER Office of Business Informatics (OBI) or management, the FDA's Systems Management Center, and/or the FDA Privacy Office. Privacy Office contact information is available on FDA's internet and intranet. Under federal policy, all agency personnel are obligated to rapidly report actual or suspected breaches to the FDA SMC.
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.	To ensure accuracy and relevancy of their PII, CDER Splunk Cloud users may correct/update their information themselves. Their PII is relevant as necessary to be authenticated and granted access to the system. Relevancy is further ensured through the design of the system to gather only the necessary PII. This assessment also enforces collection of only the PII that is essential. Integrity and availability are protected by privacy and security controls selected and implemented during providing the system with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. CDER performs annual reviews to evaluate user access. Data integrity and availability are also supported by information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified during system use are addressed when discovered.
PIA 38:	Identify who will have access to the PII in the system.	Users 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.	System Administrators: Required to configure user accounts, including FDA email addresses and user identification numbers, to facilitate authorized access to the CDER Splunk system. Authorized Users: FDA employees and designated contractors with appropriate clearance are permitted to utilize the CDER Splunk system for monitoring user login activities and system usage data. This access is granted for the purposes of troubleshooting and analyzing system performance metrics. Developers (FDA Employees and Contractors): Authorized to view personally identifiable information (PII) within the system logs to verify the accurate display of information on monitoring dashboards. Contractors: FDA Direct Contractors are authorized users, system administrators and developers.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to the CDER Splunk Cloud System is strictly controlled and managed by authorized systems administrators. Access is granted solely on the basis of legitimate need, specifically to individuals who are required to review submissions. The account creation process adheres to a rigorous internal approval protocol, which includes the following steps: The employee's supervisor must provide written justification to the CDER Splunk Cloud administrators, detailing the specific need for system access. A Role-Based Access Control (RBAC) form is submitted for review. The RBAC form must be approved by either an Office of Business Informatics (OBI) Splunk Full-Time Employee (FTE) or the Contracting Officer's Representative (COR) before access is granted. It is important to note that the CDER Splunk Cloud System is restricted to internal users only; no external users are permitted access to this 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.	User-level authorization and authentication systems are in place regarding internal users. Internal users may request access to PII in the system to perform their official duties and must obtain supervisor approval. Via technical role-based account settings, internal users may only (no external users) access their own PII that they submit when accessing the CDER Splunk Cloud system.
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.	FDA personnel including Direct Contractors are required to complete FDA's mandatory security and privacy awareness training annually.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	A training session, as well as user guide showing how to use CDER Splunk Cloud system are provided to all users of the system.
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).	FDA maintains records in accordance with the following Nation Archives and Records Administration (NARA) General Records Schedules (GRS): GRS 3.2: Information System Security Records Item 30: System Access Records – systems not requiring special accountability for access. The GRS disposition: Temporary. Authority is DAA-GRS¬2013-0006¬0003 with the records being destroyed when business use ceases. Item 40: System backups and tape library records – incremental backup files. The GRS disposition: Temporary. Authority is DAA-GRS¬2013-0006¬0005 with the records being destroyed when superseded by a full backup, or when no longer needed for system restoration, whichever is later.
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 applied include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Applied technical safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include maintenance of data servers 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:**	6/13/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/13/2025
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:**	7/16/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 7/16/2025 The PIA was reviewed outside of the tool due to sync issues. We can now approved it in Archer 4.0.	**# of Days - APA Review:**	33

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/16/2025
SAOP Review Comments:	7/16/2025 Approved on behalf of the SAOP.	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/16/2025 9:26 AM	BLAND, CRYSTAL	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	7/16/2025	7/16/2024 This PIA was reviewed and approved outside of the tool due to sync issue. Attached is a copy of the Approved PIA.	7-15-2025 CDER Splunk Cloud PIA_SAOP Approved.pdf