PTA / PIA: FDA - SBOM CVS - QTR2 - 2025 - FDA4925159

Created Date: 5/23/2025 12:36 PM Last Updated: 6/24/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - SBOM CVS - QTR2 - 2025 - FDA4925159	**PTA / PIA ID:**	3213571
Component Name:	FDA - CDRH Software Bill of Materials Completeness and Vulnerability Scanner	**ATO Boundary Name:**	CDRH Reporting and Collection Tools
Overall Status:	Complete	**# of Days - Open:**	36
Submitter:		**Submit Date:**	5/19/2025
Next Assessment Date:	06/23/2028	**Expiration Date:**	6/23/2028
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.	Initiation
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.	1/22/2023
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	Jonathan Adams
PTA 01A:	POC Title and Organization	System Owner CDRH/OSPTI
PTA 01B:	POC Email Address	jonathan.adams@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-2604
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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 purpose of the Center for Devices and Radiological Health (CDRH) Software Bill of Materials (SBOM) Completeness and Vulnerability Scanner (CVS) is to allow an SBOM document ingestion through an interface, validate the SBOM for attributes completeness against the National Telecommunications and Information Administration (NTIA) Framing document criteria, and identify, assess, and report vulnerabilities in the SBOM(s) to support compliance and security across software components. The relationship of this component CDRH SBOM CVS to other Food and Drug Administration (FDA) systems/components/information collections is that it is a component of CDRH Reporting and Collection Tools (RCT), CDRH Enterprise Datahub (CEDh). CVS may connect to another component under CEDh named Pyramid Analytics in order to provide data visualization. There are no external system connections. The key functional elements of the system include Vulnerability data ingestion and harmonization, SBOM data ingestion, SBOM and vulnerability data comparisons and Report generation. System users consist of CDRH Reviewers, Office of Strategic Partnerships and Technology Innovation (OST)/Cybersecurity Team members, Super Users, Developers, and Admins. All users are internal to FDA.

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.	The types of information collected into the system are derived from three main sources: the uploaded Software Bill of Materials (SBOM) document, third-party vendor MedCrypt's data feed, and third-party vendor Dark Sky's data feed. MedCrypt and Dark Sky data feeds include alias data tables and vulnerability data tables. These data feeds are stored in the AWS S3 bucket for a minimum of three years. While MedCrypt does not have any PII, Dark Sky's tables include names of third-party contributors, as well as banned entities/names. Both the contributor names and banned entities constitute as PII, but they are only stored in the system and do not undergo processing. The uploaded Software Bill of Materials (SBOM) consists of various details, which include but are not limited to: Author Name, Timestamp, Type, Component Name, Version String, Supplier Name, Cryptographic Hash, Unique Identifier (The unique identifier is NOT in reference to a person or individual. This Unique Identifier is related to a number associated with a technology e.g., Universal Unique Identifier (UUID)). Relationships, License and Copyright Holder. The SBOM details and alias-vulnerability feeds converge to create attribute completeness reports and vulnerability reports, which are stored in the CVS database for a minimum of three years. The CVS database may also connect to Pyramid Analytics (a sister component under CDRH RCT CEDh), where it may be stored for a minimum of three years. Users' FDA email addresses may be visible in activity logs and user lists and may be stored for three years. FDA email addresses constitute as PII. The system will be accessed via the internal URL using the single sign on process. The URL is currently being developed, and this PIA will be updated to include the URL once the URL is complete.
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.	The information about contributor names and banned entities is collected and/or maintained as it is part of the Dark Sky feed. Efforts are in place to determine if Dark Sky may be able to remove these specific PII data points altogether from the feed. The SBOM document and third-party vendor data feed ingestions are the foundation for the system's function. FDA email addresses are a requirement for Single Sign On / access and authentication.
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).	Component development in progress. URL has not been determined yet.
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 allow user groups an access point to upload SBOMs, generate analysis reports, and view system activity. The following categories of individuals have access to the website: CDRH Reviewers, OST/Cybersecurity Team members, Super Users, Developers, and Administrators. All users are internal to FDA. The URL is only accessible to users with FDA email addresses.
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.	Biographical Information Name Contact Information Email Address (Business)

PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors 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.	5,000 – 9,999
PIA 25:	For what primary purpose is the PII used?	The names appearing within data feeds are a part of the foundational data set. FDA email addresses are a function of access and authentication. They are used as identifiers within the system.
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: The Federal Food, Drug, and Cosmetic Act, section 519(f). The Medical Device Amendments to the Food Drug and Cosmetic Act, including the Medical Device Amendments 21 U.S.C. sections 360, 360c, 360e, 360i, 360j, 360l, 510(k), 515(c), 515(d), 515(f), 519, 520(g), 520(m), and 564. Safe Medical Device Act of 1990 (SMDA), 21 U.S.C. 301, 42U.S.C. 263b-n. Medical Device Reporting regulations at 21 CFR 803, 803.32, and 803.40; 21 U.S.C. 352, 360, 360i, 360j, 371, 174. The Radiological Health regulations CFR 1002.1(c)(4), 1002.10-1002.13, 1002.20, 1020.30(d), and 1020.30(d)(1), as well as Table 1 in 21 CFR 1002.1(b); 21 U.S.C. 352, 360, 360i, 360j, 360hh-ss, 371, 174.
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 Non-Government Sources Other
PIA 30A:	Identify the “other” sources of PII in the system not mentioned in the above list.	The PII from "Other Non-Government" source are last name, first name appearing in a dataset pulled by FDA from a commercial vendor called Dark Sky Technology. Dark Sky's dataset has 2 columns/fields indicating full names of "contributors" (likely contributors of said dataset) and "banned entities" (likely names of persons banned from particular access). While stored only, both the column/fields are not used for application functions.
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.	An OMB information collection approval number is not required for SBOM and CVS. Information is obtained from already existing previously collected information. New information will not be collected using new standard forms.
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 is no option to object to or opt-out of the information collection because the PII data is intrinsic to a third-party vendor feed or system access functions.
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.	There is no process to notify of obtain consent from individuals whose PII is in the system when major changes occur in the system because the PII data is intrinsic to a third-party vendor feed or system access functions.
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.	For the PII data (contributor names and banned entities names) there is no process to resolve individuals concerns because it is intrinsic to a third-party vendor feed or system access functions. FDA employees with concerns may seek assistance via FDA's Employee Resource Information Center (ERIC), FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and the FDA Privacy Office.
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.	For the PII data (contributor names and banned entities names) there is no process in place for periodic reviews of PII because the PII data is intrinsic to a third-party vendor feed. For FDA email addresses: 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 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. CDRH performs semi-annual reviews to evaluate user access.
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.	Users: A subset of users view FDA email addresses in order to identify tasks performed by other users for data analysis purposes. Administrators are responsible for system configuration, audit logs, and account management within applicable modules; directly allowing access to view FDA email addresses. Developers: The PII information within the data feeds are stored within a backend S3 bucket, which mainstay developers will have access to throughout the system's lifecycle. Developers are also privy to users lists for configuration purposes. Contractors: The application development team currently consists of contractors.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The agency uses enterprise-wide controls. Procedures include separation of duties between system administrators, change control personnel, users, and developers; access to the application at any level must first be reviewed and approved by management. Access to the system is granted via Active Directory groups by formal role-based access control (RBAC) process. FDA email addresses may be viewed by all specific user groups for work purposes. Data feed raw data with PII is accessible only to Developers.
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.	Access approvals are implemented via technical permission settings. CDRH Reviewers, OST/Cybersecurity Team members, and Super users will only have access to data meeting the criteria of the analysis they need to perform. The only other users with access to PII would be administrators and developers, and access would only be required when modifying or developing the system. Individuals in these roles would only be authorized to access PII as needed to accomplish the specific tasks they have been assigned.
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 must conduct 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 Information Management and Technology (OIMT) verifies that training has been successfully completed.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	System/system component/information collection users may also receive the following additional training/materials: Records Management Training Admin and user guides and manuals Privacy guidance available on the FDA intranet and from Privacy staff
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).	For the contributor names and banned entities PII in the system, the current retention schedule is FDA File Code 7222, Database Records, National Archives and Records Administration (NARA) Approval N1-88-07-2. Retention is temporary, with cutoff after the establishment goes out of business or the product is no longer commercially marketed, and the records would be deleted or destroyed after ten years after cutoff or when no longer needed for legal, research, historical or reference purposes, whichever is the latest. While credentials are managed by Active Directory, FDA email addresses appear in the system and remain available as a logged item according to NARA 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.	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:**	5/19/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/23/2025
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:**	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/5/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	13

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	19

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/24/2025 2:57 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	5/27/2025	5-27-2025 Per FDA's Email, The PIA is experiencing an Archer error with question General 03: Q-3 “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 1/22/2023. 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.	5-27-2025 EMAIL_PIA in Queue (CDRH Software Bill of Materials Completeness and Vulnerability Scanner).pdf CDRH Software Bill of Materials Completeness and Vulnerability Scanner_SOP Approved.pdf