PTA / PIA: FDA - DCS - QTR4 - 2025 - FDA4977989

Created Date: 10/8/2025 12:22 PM Last Updated: 11/20/2025 11:29 AM

General Information

PTA / PIA Name:	FDA - DCS - QTR4 - 2025 - FDA4977989	**PTA / PIA ID:**	3891346
Component Name:	FDA - HFP Document Control System	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	44
Submitter:		**Submit Date:**	11/18/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
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.	10/20/2022
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	Carrol Burgundy
PTA 01A:	POC Title and Organization	Privacy Officer, HFP/OPIE
PTA 01B:	POC Email Address	carrol.burgundy@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-2158
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.	N/A - This is the initial PTA/PIA for the system.
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.	Document Control System (DCS) is a document repository for use to maintain a history of relevant documents such as case law, communication, etc. for cosmetics and colors. These documents are stored in digital files in an Oracle database and as a reference for the location of the physical files and folders. DCS users (FDA employees only) can also attach metadata such as document author, publication date, or category to each document that is stored within the Oracle database. DCS users the Office of Cosmetics and Colors (OCAC) employees, who add, edit and/or search for documents related to cosmetics and colors. The Office of Cosmetics and Colors (OCAC) uses two web applications which are only accessible to cosmetic companies (considered members of the public) and authorized FDA personnel (permanent employees and direct contractors). The system containing both applications is referred to as OCAC Applications (OCAC Apps). The OCAC Apps/web applications includes the Voluntary Cosmetic Registration Program (VCRP) and the Document Control System (DCS).
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.	FDA uses DCS to store internal communications, documents, and reports related to cosmetics. DCS collects and maintains the following types of information: (a) Personally Identifiable Information (PII) - document author and document reviewer first and last names. Other forms of PII may include first and last names, business contact information including work e-mail addresses, telephone numbers, and mailing addresses that are contained in the documents themselves. The PII is retained in DCS indefinitely and is not shared with any system or organization. All personally identifiable information (PII) and non-PII DCS is stored in the Oracle database which is part of the OCAC Apps system and is covered by the security and privacy assessments and authorization to operate documentation for the system. DCS is Single Sign On (SSO), and PIV enabled. The system has implemented a multifactor authentication via alternate PIV cards for network access to privileged accounts. The FDA uniquely identifies and authenticates organizational users. For PIV authenticated system, PIV credentials are based on user's certification which are also unique. DCS collects the following non-PII: document folder, document name, document type, status, due date, publication, date, affiliation, internal reference number, whether a response is needed, keywords, and memoranda that summarize a document.

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.	Yes, but the user credentials are maintained in a separate system (e.g., Active Directory (AD), AMS) and not collected or maintained by this system. The system providing credentials is EASE.
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.	DCS system collects business contact information, which is considered PII. DCS collects the following PII information: (a) names of FDA employees and business partners/contacts; (b) work e-mail addresses; (c) telephone numbers and (d) mailing addresses. The PII data is not shared with any other system or organization. FDA created DCS to enable the Office of Cosmetics and Colors to easily file and track documents. DCS stores files (including information about the physical files) for archival purposes. FDA users can categorize, attach keywords, apply other metadata, and search for documents in the system. All DCS users are FDA employees who connect via a single sign-on process using multi-factor authentication. Records are retrieved by the Document ID number assigned by the database; users can also organize files into folders within the system to allow easier retrieval.
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://hfpappinternal.fda.gov/scripts/ocacapp/dcs/**
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 system is to maintain a history of relevant documents such as case law, communication, etc. for cosmetics and colors. The following categories of individuals have access to the website: FDA employees/contractors Users access the website via an Intranet URL, that is not accessible by the public.
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 (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing 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 primary purpose of using PII in the system is to grant access to users to add, edit and/or search for documents related to cosmetics and colors. Contact information may be included (email address, phone number, mailing address) in the documents themselves. This information is utilized to review cosmetic documents related to manufacturing, packaging, and product formulas.
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.	DCS is an internal-only document repository that provides a general administrative and support system. It is authorized by 5 U.S.C. 301, Federal Information Processing Standards (FIPS) 199 and NIST SP 800-60 Rev. 5
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 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.	No information is collected from the public.
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 opt-out of the collection of PII data for DCS users. Submitters 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 DCS. DCS is a document storage repository for documents such as letters from elected officials (which are a part of the public record) or letters/documents from public citizens which are not part of the public record. As these submissions to the FDA are voluntary, individuals are aware that they are providing their PII to the agency.
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 FDA changes its practices with regard to 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 email 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 DCS as DCS is not available or accessible to the public. 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-employees or Direct Contractors only), the Cybersecurity and 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 without delay to FDA's Cybersecurity and Infrastructure Operations and 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 agency reviews PII during the approval and certification process of system. Annual reviews are conducted to evaluate user access. Availability, relevancy, accuracy, and integrity of PII about FDA employees is addressed at the source system, EASE, where reviews and controls are applied pursuant to security and privacy assessments of that system as well as under organizational business practices. 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.
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.	The reason the following groups need access to PII is: Users: Search for documents related to cosmetics and colors. Administrators: Add, edit and/or search for documents related to cosmetics and colors. Developers: For developing and testing new software releases and troubleshooting errors. Some of the developers are Direct Contractors. Contractors: Direct contractors who perform administrative, development, testing, and maintenance purpose.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users who require access to the PII in the system need to obtain supervisory approval and sign off on a Rules of Behavior form before access is granted. The Rules of Behavior for using DCS are clarified and mandated by HHS guidelines and security documentation. There are two ways to request access to the applications: the user emails the business owner/IT Technical Lead or submits a request online through the 'Request Access' application option. Misuse of data in DCS is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and are adequately trained regarding the security of their systems.

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.	Role based security controls ensure that each user role is appropriately assigned at the individual level in accordance with an individual user's need-to-know and least-access-privileges in regard to official duties such that each user sees/accesses only that data that is essential to complete his/her job. The user's supervisor will indicate on the account creation form the minimum necessary information system access that is required for the user to complete his/her job. The agency reviews the access list for the information system on a quarterly basis. During this process users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the 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.	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 Information Management and Technology (OIMT) verifies that training has been successfully completed by all FDA employees and direct contractors.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	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 Information Management and Technology (OIMT) verifies that training has been successfully completed by all FDA employees and direct contractors.

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).	Records for DCS consisting of cosmetic ingredient reviews, establishment inspection reports, warning letters, and lawsuits/legal discussions are maintained under NARA citation N1-088-09-1. The disposition is temporary with the cutoff being at the end of the fiscal year and the records are destroyed deleted 10 years after the cutoff date. Written reports within DCS are covered under NARA citation NC 1-88-07-2 and the records are transferred to NARA 20 years after the cutoff date. Internal communications within DCS are covered under NARA N1-088-06-3 and are transferred to NARA 20 years after the cutoff date. Administrative safeguards include user training on PII and implementation of Need to Know and Minimum Necessary principles when awarding access. Technical Safeguards include the use of two-factor access authentication, device disk encryption, firewalls, virtual private network (VPN) and network monitoring and intrusion detection tools. Physical controls include the location of all system servers located at FDA 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.
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: the use of two-factor access authentication, device disk encryption, firewalls, virtual private network (VPN) and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at FDA 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:**	11/18/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	11/18/2025
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/19/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/19/2025 All comments have been addressed. This PIA is ready for SAOP review and approval. 11/17/2025 Please see comment and update accordingly: PIA-22: Per PTA-5, please select the following PII elements Email Address (Business); Mailing Address (Business); and Phone Numbers (Business).	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	11/20/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	1

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/20/2025 11:01 AM	BAUR, VANESSA	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	VILLAFUERTE, NESTOR	10/10/2025	Does the system have an updated ATO date?	
PTA 01	BLAND, CRYSTAL	11/17/2025	11/17/2025 Per FDA email on 10/8/2025 "The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. **The ATO date is 10/20/2022.** At this time, we are unable to update Archer to reflect the correct answer “Yes.”"	1--8-2025 EMAIL_RE_ HFP Document Control System FDA- (FDA - DCS - QTR4 - 2025 - FDA4977989).pdf
PIA 22	BLAND, CRYSTAL	11/17/2025	Per PTA-5, please select the following PII elements Email Address (Business); Mailing Address (Business); and Phone Numbers (Business).	