


General Information		
<b>PTA / PIA Name:</b>	FDA - FDCC - QTR2 - 2025 - FDA4919126	<b>PTA / PIA ID:</b> 3126805
<b>Component Name:</b>	FDA - HFP Food Colors and Cosmetics Web Modules	<b>ATO Boundary Name:</b> CBER Office of Regulatory Operations
<b>Overall Status:</b>	Complete 	<b># of Days - Open:</b> 8
<b>Submitter:</b>		<b>Submit Date:</b> 5/5/2025
<b>Next Assessment Date:</b>	N/A	<b>Expiration Date:</b> 1/1/2100
<b>Office:</b>		<b>OpDiv:</b> FDA
<b>Security Categorization:</b>	Moderate	
<b>Make PIA available to Public?:</b>	Yes	<b>PIA Required:</b> Yes
<b>General 01:</b>	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
<b>General 02:</b>	Is this a FISMA-Reportable system?	Yes
<b>General 03:</b>	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
<b>General 04:</b>	ATO Date or Planned ATO Date.	10/20/2022
<b>General 05:</b>	Is the system or electronic information collection, agency or contractor operated?	Agency
<b>History Log:</b>	<a href="#">View History Log</a>	

Privacy Threshold Analysis		
<b>Privacy Threshold Analysis</b>		
<b>PTA 01:</b>	Point of Contact (POC) Name	Amelia Morris
<b>PTA 01A:</b>	POC Title and Organization	Chemist, OC/FDA
<b>PTA 01B:</b>	POC Email Address	amelia.morris@fda.gov
<b>PTA 01C:</b>	POC Phone Number	240-402-1118
<b>PTA 02:</b>	Indicate the following reason(s) for this PTA. Choose from the following options.	New
<b>PTA 03:</b>	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 Food Colors and Cosmetics Web Page Modules (FDCC) application is to act as a platform where multiple HFP offices can post critical data set information as required to support regulations, guidance documents, public comment and response to proposed and final rules, Government Accountability Office (GAO) findings, Memorandum of Understanding (MOUs) with other agencies (e.g., environmental decisions (see 40 Code of Federal Regulation (CFR) 1506.6(b) and 21 CFR 25.10(a)), food contact notifications (see 65 Federal Registrar (FR) 43269 7/13/2000 and 67 FR 35724, 5/21/2002), Generally Recognized As Safe (GRAS) notifications (see 75 FR 81536 at p. 81539), and the GAO 2009 report to prevent seafood fraud to the FDA Web site. The FDA provides the information on the web as proactive release to reduce FOIA requests and as a response to the FDA Transparency Initiative.

The FDCC system is available to the public and doesn't require an account. The system has an administration component, which includes a wizard that allows authorized FDA users to upload a spreadsheet and specify how the data in that spreadsheet is to be presented to the viewer.

FDCC includes two user modules. Users of the external module include external stakeholders throughout the Food, Drug, Cosmetic, and Medical Device industries, who do not require a user account to access the system. Users of the internal module is limited to a very small group of Administrators and Investigators (FDA Employees) and Developers (FDA Direct Contractors).

Note: FDCC is a component of the system HFP Cosmetic and Colors Applications (HCCA). The purpose(s) of the Cosmetic and Colors Applications (HCCA) system is to review samples of synthetic colors dyes and approve them for use in foods, drugs, and cosmetics.

**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.

FDCC collects and maintains the following personally identifiable information (PII) in professional capacity about FDA employees (permanent and Direct Contractors): (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. The FDA system providing employee data is the Enterprise Administrative Support Environment (EASE) system (the subject of a separate assessment). Employee data is used to log on authorized users automatically and securely.

HFP FDCC does not collect any PII about external users of the system.

Non-PII collected and maintained in the system includes Official Public Information Dissemination.

<b>PTA 05A:</b>	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.
<b>PTA 05C:</b>	Please identify the system that maintains the user credentials or controls access to this system.	The FDA system providing employee data is the Enterprise Administrative Support Environment (EASE) system (the subject of a separate assessment).
<b>PTA 06:</b>	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.	<p>The purpose of the FDCC component is to act as a platform where multiple HFP offices can post critical information such as that mandated by Congress, regulation, guidance documents, or other agreement, to the FDA Web site. The system collects information/data that allow the public and internal FDA users to search for information on regulations, guidance, and FDA regulated products. Via FDCC application, FDA provides information to accommodate Electronic Freedom of Information Act (e-FOIA) and the FDA Transparency Initiative.</p> <p>The FDCC component is Single Sign On (SSO), and Personal Identity Verification (PIV) card enabled for internal users. 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. Users of the system include Administrators and Investigators (FDA Employees) and Developers (FDA Direct Contractors). FDCC utilizes PIV cards and Single Sign On (SSO). The authenticator is managed by Active Directory and all access is managed and granted through PIV/SSO.</p> <p>Users of the external module include external stakeholders throughout the Food, Drug, Cosmetic, and Medical Device industries that need to view critical data set information posted via the application as listed above and therefore do not require a user account to access the system.</p>
<b>PTA 07:</b>	Does the system collect, maintain, use, or share PII?	Yes
<b>PTA 08:</b>	Does the system include a website or online application?	Yes
<b>PTA 08A:</b>	Provide the URL(s).	<a href="https://www.cfsanappsexternal.fda.gov/scripts/fdcc/">https://www.cfsanappsexternal.fda.gov/scripts/fdcc/</a> <a href="https://cfsanappsinternal.fda.gov/scripts/fdcc/">https://cfsanappsinternal.fda.gov/scripts/fdcc/</a> <a href="https://cfsanappsinternal.fda.gov/scripts/fdcc/admin/">https://cfsanappsinternal.fda.gov/scripts/fdcc/admin/</a>
<b>PTA 08B:</b>	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

<b>PTA 09:</b>	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.	<p>The purpose of the website is to act as a platform where multiple HFP offices can post critical information such as that mandated by Congress, regulation, guidance documents, or other agreement, to the FDA Web site. The system collects information/data that allow the public and internal FDA users to search for information on regulations, guidance, and FDA regulated products. Via FDCC application, FDA provides information to accommodate e-FOIA and the FDA Transparency Initiative.</p> <p>The FDCC system includes a website or online application that is accessible to the public.</p> <p>Users access the website via public Uniform Resource Locator (URL).</p>
<b>PTA 10:</b>	Does the website have a posted privacy notice?	Yes
<b>PTA 11:</b>	Does the website contain links to non-federal government websites external to HHS?	No
<b>PTA 12:</b>	Does the website use web measurement and customization technology?	Yes
<b>PTA 12A:</b>	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
<b>PTA 13:</b>	Does the website have any information or pages directed at children under the age of thirteen?	No
<b>PTA 14:</b>	Does the system have a mobile application?	No
<b>PTA 20:</b>	Are any third-party websites or applications (TPWA) associated with the system?	No
<b>PTA 21:</b>	Does this system use artificial intelligence (AI) tools or technologies?	No

### Privacy Impact Assessment

#### Privacy Impact Assessment

<b>PIA 22:</b>	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	<p>Biographical Information</p> <p style="padding-left: 20px;">Name</p> <p>Contact Information</p> <p style="padding-left: 20px;">Email Address (Business)</p> <p style="padding-left: 20px;">Mailing Address (Business)</p> <p style="padding-left: 20px;">Phone Numbers (Business)</p>
<b>PIA 23:</b>	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
<b>PIA 24:</b>	Indicate the approximate number of individuals whose PII is maintained in the system.	<100
<b>PIA 25:</b>	For what primary purpose is the PII used?	The primary purpose of using PII in the system is to validate accounts of FDA personnel.
<b>PIA 26:</b>	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.

<b>PIA 28:</b>	Identify legal authorities, governing information use and disclosure specific to the system and program.	<p>The legal authorities that govern information use and disclosures specific to the system and program are :</p> <p>Federal Information Processing Standards (FIPS) 199</p> <p>National Institute of Standards and Technology Special Publications (NIST SP) 800-60 Rev. 1, Volumes I and II.</p> <p>40 CFR 1506.6(b)</p> <p>21 CFR 25.10(a)</p> <p>65 FR 43269 7/13/2000 and 67 FR 35724, 5/21/2002</p> <p>GRAS notifications (see 75 FR 81536 at p. 81539)</p>
<b>PIA 29:</b>	Are records in the system retrieved by one or more PII data elements?	No
<b>PIA 30:</b>	Identify the sources of PII in the system.	<p>Government Sources</p> <p>Within the OPDIV</p>
<b>PIA 31:</b>	Is there an Office of Management and Budget (OMB) information collection approval number?	No
<b>PIA 31B:</b>	Explain why an OMB information collection approval number is not required.	Does not meet requirements for PRA.
<b>PIA 32:</b>	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
<b>PIA 33:</b>	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Mandatory
<b>PIA 33A:</b>	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	All Health and Human Services (HHS) employees who uses this system, must provide PII mandatory in order to have access to system or non-disclosure would result in civil or criminal penalties.
<b>PIA 34:</b>	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.	<p>As submission of data is mandatory under Code of Federal Regulations environmental decisions (see 40 CFR 1506.6(b) and 21 CFR 25.10(a)), food contact notifications (see 65 FR 43269 7/13/2000 and 67 FR 35724, 5/21/2002), GRAS notifications (see 75 FR 81536 at p. 81539), and the GAO 2009 report to prevent seafood fraud to the FDA Web site, there is no process for users to opt out of providing their PII. While FDA requires that regulated entities supply the PII of a point of contact, that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity.</p> <p>The FDA requires the contact information of the employees and contractors to validate access to the system.</p>

<p><b>PIA 35:</b></p>	<p>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.</p>	<p>If FDA changes its practices regarding the collection or handling of PII related to the website, FDCC 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.</p>
<p><b>PIA 36:</b></p>	<p>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.</p>	<p>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).</p> <p>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).</p>
<p><b>PIA 37:</b></p>	<p>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.</p>	<p>The agency reviews PII during the approval and certification process.</p> <p>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. The individual is responsible for providing accurate information. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access).</p> <p>HFP performs annual reviews to evaluate user access. One of the controls includes 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.</p> <p>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.</p> <p>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.</p>

<b>PIA 38:</b>	Identify who will have access to the PII in the system.	<p>Users</p> <p>Administrators</p> <p>Developers</p> <p>Contractors</p>
<b>PIA 38A:</b>	Select the type of contractor.	HHS/OpDiv Direct Contractors
<b>PIA 38B:</b>	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
<b>PIA 39:</b>	Provide the reason why each of the groups identified in 38 needs access to PII.	<p>Users: Receive, review, manage and track submissions.</p> <p>Administrators: Administer the system, manage workflow and system access. Some administrators are direct contractors.</p> <p>Developers: For developing and testing new software releases and troubleshooting errors. Some of the developers are Direct Contractors.</p> <p>Contractors: Direct contractors who perform administrative, development, testing, and maintenance purpose.</p>
<b>PIA 40:</b>	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 before access is granted. There are two ways to request access to the applications: the user emails the business owner/ Information Technology (IT) Technical Lead or submits a request online through the 'Request Access' application option. 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.
<b>PIA 41:</b>	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 regarding official duties such that each user sees/accesses only that data that is essential 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.
<b>PIA 42:</b>	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 individuals successfully complete the training.

<p><b>PIA 43:</b></p>	<p>Describe the training system users receive above and beyond general security and privacy awareness training.</p>	<p>HFP Web Page Modules (FDCC) users are instructed on system use and must sign a non-disclosure agreement before being granted access to the office’s online application (FDCC).</p> <p>Personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available, and personnel may request additional privacy guidance from HFP’s privacy office.</p>
<p><b>PIA 44:</b></p>	<p>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).</p>	<p>The records for HFP’s Web Page Modules (FDCC) fall under General records Schedule (GRS) 3.1 item 51. In addition to GRS 3.1, records in FDCC utilize HFP file codes 10100, 10200, and 9100. The cutoff for these records is when the critical data set information as required to support regulations, guidance documents, public comment, and response to proposed and final rules, GAO findings, MOUs with other agencies are no longer available or if the information has been rescinded. The disposition schedule states the records are to be destroyed when they are no longer needed for legal, research, or other regulatory purposes, or 3 years after the cutoff, whichever is latest.</p>
<p><b>PIA 45:</b></p>	<p>Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.</p>	<p>Administrative safeguards include user training on PII and implementation of Need to Know and Minimum Necessary principles when awarding access.</p> <p>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.</p> <p>Physical controls include the location of all system servers located at FDA facilities protected by guards, locked facility doors, and climate controls.</p> <p>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.</p>

## Review and Comments

### OpDiv Privacy Analyst Review

<b>Privacy Analyst Review Decision:</b>	Approved	<b>Privacy Analyst Review Date:</b>	5/5/2025
<b>Privacy Analyst Review Comments:</b>		<b># of Days - PA Review:</b>	0

### SOP Review

<b>SOP Review Decision:</b>	Approved	<b>SOP Review Date:</b>	5/5/2025
<b>SOP Review Comments:</b>		<b># of Days - SOP Review:</b>	0

### Agency Privacy Analyst Review

<b>Agency Privacy Analyst Review Decision:</b>	Approved	<b>Agency Privacy Analyst Review Date:</b>	5/6/2025
<b>Agency Privacy Analyst Review Comments:</b>	<p>Reviewer: Crystal Bland</p> <p>5/6/2025 all comments seemed to be addressed. Submitting for SAOP review and approval.</p> <p>5/2/2025 Please see comments and update accordingly.</p> <p>PTA-1-1C: Must provide POC information prior to PIA and ATO approval.</p> <p>PTA-12C: The response provided for PTA-12C should be included in PTA-9 response. The question being ask here is what PII is the Session Cookie collecting. If no PII is being collected then update PTA-12A to Session Cookie-Does Not Collect PII.</p> <p>PIA-22: Per PTA-5, work email is collected, please update your selection to Email Address (Business). Is Mailing Address Personal or Business? If Business then update your selection to Mailing Address (Business).</p>	<b># of Days - APA Review:</b>	1

### SAOP Review

<b>SAOP Review Decision:</b>	Approved	<b>SAOP Review Date:</b>	5/7/2025
<b>SAOP Review Comments:</b>		<b># of Days - SAOP Review:</b>	1

### SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/7/2025 10:46 AM	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	5/1/2025	<p>5-1-2025 Couldn't attached email or copy of PIA, received error "invalid size." Email stated the following:</p> <p>The PIA is experiencing an Archer error with Question #3 of the general information.</p> <p>Q-3 "Does the system have or is it covered by a Security Authorization to Operate (ATO)?"</p> <ul style="list-style-type: none"><li>The FDA instance of Archer is automatically entering the answer "No," which is incorrect. The ATO date is 12/23/2022.</li><li>At this time, we are unable to update Archer to reflect the correct answer "Yes."</li></ul> <p>The FDA Archer Team is aware of this occurrence and is working on a solution.</p>	
PTA 01	BLAND, CRYSTAL	5/1/2025	Must provide POC info (Name) prior to PIA and ATO approval.	
PTA 01A	BLAND, CRYSTAL	5/1/2025	Must provide POC title and organization info prior to PIA and ATO approval.	
PTA 01C	BLAND, CRYSTAL	5/1/2025	Must provide POC phone number prior to PIA and ATO approval.	
PTA 12C	BLAND, CRYSTAL	5/2/2025	The response provided for PTA-12C should be included in PTA-9 response. The question being ask here is what PII is the Session Cookie collecting. If no PII is being collected then update PTA-12A to Session Cookie-Does Not Collect PII.	
PIA 22	BLAND, CRYSTAL	5/2/2025	Per PTA-5, work email is collected, please update your selection to Email Address (Business). Is Mailing Address Personal or Business? If Business then update your selection to Mailing Address (Business).	