PTA / PIA: FDA - APPCMD - QTR2 - 2025 - FDA4917497

Created Date: 4/25/2025 11:34 AM Last Updated: 6/24/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - APPCMD - QTR2 - 2025 - FDA4917497	**PTA / PIA ID:**	3087171
Component Name:	FDA - HFP App Command	**ATO Boundary Name:**	CFSAN Food Safety & Nutrition Submission Applications
Overall Status:	Complete	**# of Days - Open:**	70
Submitter:		**Submit Date:**	5/20/2025
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)?	No
General 04:	ATO Date or Planned ATO Date.	12/23/2022
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	Wenmin Chen
PTA 01A:	POC Title and Organization	IT PM, OC/FDA
PTA 01B:	POC Email Address	wenmin.chen@fda.gov
PTA 01C:	POC Phone Number	240-402-0730
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.	This Application Command System was a part of the HFP Food Safety and Nutrition Submission Application (CFSNSA) system. However, this system is no longer under the CFSNSA system. It is now a standalone system with a separate PIA.
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 FDA HFP App Command (APPCMD) is to provide basic operations and maintenance support which includes emergency and minor releases. APPCMD is a security application module used to control security for all the HFP developed Coordinated Outbreak Response, Evaluation (CORE) applications. It currently works with Food Code Reference System (FCRS) and Seafood APPCMD. The system collects business contact information, which is considered PII. APPCMD collects the following PII information: (a) names of FDA employees and business partners/contacts; (b) work email addresses; (c) work telephone numbers; and (d) work mailing addresses. The PII data is not shared with any other system or organization. APPCMD does not collect any non-PII data. System “users” consist of FDA employees and Direct Contractors.

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.	APPCMD collects from FDA employees and Direct Contractors the following PII: (a) first and last name; (b) FDA email address; (c) phone number; and (d) mailing address. The PII is in professional capacity and not shared with anyone or system. APPCMD does not collect any non-PII data. APPCMD collects and maintains the following types of information: (a) Personally Identifiable Information (PII) - business contact information including work email addresses, telephone numbers, and mailing addresses. APPCMD 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. The amount of time the PII is stored in the system is: Records Schedules numbered File Code 030 and 031. DAA-GRS-2013-0006-0003 (System Access Records) Temporary. Destroy when business use ceases. A-GRS-2013-0006-0004: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
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

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 FDA employees and Direct Contractors is collected and/or maintained to have access and use of the application. No information is shared with any other source. Application Command (APPCMD) is a security application module used to control security for all the HFP developed Coordinated Outbreak Response, Evaluation (CORE) applications. It currently works with Food Code Reference System (FCRS) and Seafood APPCMD. The purpose of APPCMD is to provide basic operations and maintenance support which includes emergency, and minor releases. FDA employees and Direct Contractors who access or use these applications do not use any personal identifiers to retrieve records held in APPCMD. APPCMD system 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. Users of the system include administrators (FDA Employees) and developers (FDA Direct Contractors). APPCMD 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.
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/appCmd/default.cfm
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 APPCMD is to provide basic operations and maintenance support which includes emergency, and minor releases. The following categories of individuals have access to the website include Administrators (FDA Employees) and Developers (FDA Direct Contractors). Users access the website via (public URL, Login, etc.): Login
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?	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) 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 validate accounts of FDA personnel and provide access control security for some HFP developed applications.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	None
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 U.S.C. 301, 44 U.S.C. 35, 21 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.	App Command doesn't collect PII from members of the public. This does not meet the definition of "information collection request" as defined by the Paperwork Reduction Act (PRA).
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 APPCMD users. The submission of PII is voluntary. All users of the system (FDA employees and Direct Contractors (where applicable) log time in the application and provide their PII to perform work.

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 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.	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 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.	Individuals voluntarily provide their PII. 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 while 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. HFP performs annual reviews to evaluate user access. The limited amount of PII involved is reviewed during the approval and certification process conducted for all submitted APPCMD forms.
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.	FDA employees, Administrators and Direct Contractors require access to perform system specific related duties. Users - have access to the PII for submissions they make. FDA users will have access to PII to review and manage the applications and travel transactions. Note that "FDA users" may include subject individuals, supervisors, or system administrators. Administrators - System administrators may have access to PII to conduct business functions. System administrators may have access to PII to support system administration activities. Developers - Developers may have access to PII to maintain the system and provide technical assistance to users. Contractors - Some developers and system administrators may be Direct Contractors and will have access under the same circumstances as developers
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 have supervisor approval before access is granted. 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. The users' supervisor will indicate on the account creation form the minimum 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 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.	For APPCMD, the user's supervisor indicates on the account creation form the minimum necessary system access that is required for the user to complete his/her job. Individual-level role-based access controls are applied using technical settings and multifactor user identity authentication. The agency reviews the information system access list semi-annually. During this review the agency reviews/adjusts users' access permissions and removes unneeded accounts 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 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.	FDA employees and Direct Contractors receive generalized APPCMD training and may obtain privacy guidance through 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 specific National Archives and Records Administration (NARA) records schedule is File Code 030 and 031. DAA-GRS-2013-0006-0003 (System Access Records) Temporary. The retention schedule and retention period(s) is/are: Destroy when business use ceases. A-GRS-2013-0006-0004: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
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:**	5/20/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/30/2025
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:**	10

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland (Shanai Shobowale) 6/5/2025 All comments were addressed. This PIA is ready for SAOP review and approval. 5/15/2025 See comments and update accordingly. PTA-01 - PTA-01C: Must provide POC Contact information prior to PIA and ATO approval. PIA-22: PTA-5 states "(a) Personally Identifiable Information (PII) - business contact information including work email addresses, telephone numbers, and mailing addresses." Please update or add the following selections email address (Business), Phone number (Business), and Mailing Address (Business). PIA-31B: Per PTA-5, "APPCMD collects from FDA employees and Direct Contractors" who are users of the system. Rephase the first sentence to read "App CMD doesn't collect PII from members of the public."	**# of Days - APA Review:**	6

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 2:51 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	5/15/2025	FDA Failed to provide the Point of Contact information which must be provided to approved the PIA and ATO.	HFP APP Command.pdf 5-13-2025 EMAIL_HFP App Command Privacy_Assessment.pdf
PTA 01	BLAND, CRYSTAL	5/15/2025	5/15/2025 Per FDA Email, the PIA is experiencing an Archer error with Question #3 of the general information. 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 12/23/2022. 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.	
PTA 01A	BLAND, CRYSTAL	5/15/2025	Must provide title and organization information prior to PIA and ATO Approvals.	
PTA 01C	BLAND, CRYSTAL	5/15/2025	Must provide a phone number prior to PIA and ATO approvals.	
PIA 22	BLAND, CRYSTAL	5/15/2025	PTA-5 states "(a) Personally Identifiable Information (PII) - business contact information including work email addresses, telephone numbers, and mailing addresses." Please update or add the following selections email address (Business), Phone number (Business), and Mailing Address (Business).	
PIA 31B	BLAND, CRYSTAL	5/15/2025	Per PTA-5, "APPCMD collects from FDA employees and Direct Contractors" who are users of the system. Rephase the first sentence to read "App CMD doesn't collect PII from members of the public."	