PTA / PIA: FDA - CFORCE - QTR2 - 2025 - FDA4926460

Created Date: 5/30/2025 4:37 PM Last Updated: 6/24/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - CFORCE - QTR2 - 2025 - FDA4926460	**PTA / PIA ID:**	3249711
Component Name:	FDA - HFP Workforce Management System	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	34
Submitter:		**Submit Date:**	6/12/2025
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	Fatima Dasti
PTA 01A:	POC Title and Organization	IT PM, HFP/FDA
PTA 01B:	POC Email Address	fatima.dasti@fda.gov
PTA 01C:	POC Phone Number	301-796-7898
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.	The newest version of CFORCE v3.3 introduced enhancements to the space management module by allowing offices to make space requests for incoming employees as well as the creation of an email module that allows users to send messages via email to a select group of individuals (FDA employees and Direct Contractors). The newest version also adds a travel module to integrate and automate all staff travel preparations, approvals and related processes (previously completed in PDF forms and FDA's SharePoint).
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 Food Safety and Applied Nutrition's (CFSAN) Workforce (CFORCE) system is to aid CFSAN's program alignment efforts via collection and maintenance of employee skills data. To accomplish this task, the system enables management to view employee skill sets, levels of education, and certifications both individually and aggregated across organizations and programs. The Human Resource (HR) management data is used to accurately track and maintain CFSAN personnel and positions as well as view and manage essential information related to new hires, backfills and other positions for human resource planning activities. The space management data is used to monitor office space to aid planning and assignment processes for office space and perform space analysis. The new travel module integrates and automates all travel processes currently completed in PDF forms and SharePoint (via the use of personalized user dashboards, automated workflows, automated emails, and automated e-signature functionality).
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 system collects and maintains data associated with individual federal employees including passport numbers, education records, personal email address and phone number, employee specific positions/status, name, work phone number, work e-mail, responsibilities, program involvement, skills, certifications, education status, pay plan and grade. All entries use formats such as radio buttons or drop-down menus; there are no open fields and therefore no opportunity to enter information that is not specifically solicited. Access to system uses a single sign on (SSO) approach employing multi-factor authentication; there are no system-specific authentication credentials housed in the system. Federal employees and direct contractors including system administrators and developers access this system using SSO.
PTA 05A:	Are user credentials used to access the system?	No

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 system collects data from CFSAN employees via web-based (FDA Intranet) surveys. The surveys collect only the information described such as employee position/status, name, work phone number, work e-mail, responsibilities, program involvement, skills, certifications, education status, pay plan and grade. There are no questions or fields that would permit employees to include irrelevant sensitive information such as Social Security number (SSN), health information, or financial information. CFSAN management uses this information to better align their human resources with Center priorities. System users are CFSAN personnel charged with assigning tasks and identifying resources; there are no users with any access outside of CFSAN. CFSAN employees who provide information about their knowledge, skills and abilities do not have access to others' information unless they are in those project planning roles. Users use the PII in CFORCE to identify skill gaps and better align their human resources with program priorities. Users do not retrieve information from the system by name or other unique personal identifier, and the system is not a 'system of records' under the Privacy Act. The system can only be searched by credentials (e.g., professional certifications) and qualifications. There are no system-specific authentication credentials housed in the CFORCE system. Federal employees and direct contractors including system administrators and developers access this system using SSO.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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.	Identifying Numbers Passport Number Biographical Information Name Certificates (e.g., training certificates) Education Records Employment Status/History Contact Information Email Address (Personal) Phone Numbers (Personal) 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.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	In the profile module the PII is used to help identify which employees may be appropriate for various assignments and roles based on their knowledge, skills, and abilities. The PII within the HR module is used by the Division of Workforce Management to carry out their day-to-day HR responsibilities. In the Space Management module, the PII is used for office space requests. The PII in the travel module is used to process submissions from CFSAN employees who are requesting travel through CFORCE.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	No secondary uses of the PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Government Employees Training Act (5 U.S.C. 4101 et seq); Executive Order 11348 (Providing for the further training of Government employees); 5 U.S.C. 301; and the Federal Food, Drug, And Cosmetic Act at 21 U.S.C. 379l (Education), which provides that "The Secretary shall conduct training and education programs..." for employees relating to FDA's responsibilities, and meeting this mission is facilitated by knowing the skill sets and training history of existing staff.
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.	Not required as there are no PRA requirements with this component.
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.	All PII collected (with the exception of voluntary and self-created user profiles) is directly related to essential administrative functions and users cannot opt out of having essential data maintained in the application PII collected as part of the profile module is completely voluntary for each employee.
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 a major change to CFORCE occurs, the center (CFSAN) will communicate to end users via email and/or in person notifying them of major changes to the application and the types of data being maintained.
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.	Employees have many opportunities to address any concerns about inappropriate use or disclosure of their PII. Individuals may use an Employee Resource and Information Center (ERIC) Helpdesk service, or contact Agency offices using information available on the FDA intranet and internet. These offices include the FDA Privacy office, the appropriate Information System Security Officer in FDA IT Security, the office of the responsible CFORCE system owner, the office of the direct supervisor or human resources representative. For suspected exposure, misuse of compromise of PII, all personnel must report the matter to the FDA Systems Management Center which coordinates with Privacy and Security offices to respond.

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 PII accuracy, FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. In the profile module FDA personnel voluntarily submit their PII, are responsible for providing accurate information and may independently update and correct their information at any time. In the HR module (release 2.0 and 3.0) the Division of Workforce Management monitors and maintains data daily, ensuring its accuracy. In the Space module (release 3.0) Space Management staff monitors and maintains data daily, ensuring its accuracy. And, in the Travel module (release 4.0) Program Services monitors and maintains data daily, ensuring its accuracy. Integrity is protected via restricted access granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are also protected by security and privacy controls selected and implemented in the course of 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. Relevancy is ensured by the design of the system to collect only the PII that is specifically necessary for the authorized purposes of the system and the official activities the system supports.
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?	No

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: General users only have access to their own data. Division of Workforce Management (FDA Employees) currently has access to all of the PII that will eventually be captured in CFORCE. Administrators: Administrators access PII for account management purposes. Some of the Administrators are Direct Contractors. Developers: Developers may have access to PII in the course of updating and maintaining the system. Some of the developers are Direct Contractors. Contractors: For system maintenance and account management purposes. Some of the Administrators and Developers are the Direct Contractors.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All general users must be explicitly provisioned in the application. These users will only have access to their own PII. All HR module users must be employees of the Division of Workforce Management and will be required to be approved by the Director of the Division of Workforce Management.
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 role is appropriately assigned at the individual level in accordance with need-to-know and least-access privileges in regard to official duties such that each person only sees/accesses data that is essential to the tasks they need to accomplish.
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 users are FDA employees who must complete Security Training and Privacy Awareness Training on an annual basis.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	General users are provided basic training in the profile module by the application developers via demonstration. The application developers are available for further training should it be requested. HR module and Space Management module users are given individual, in-depth training by the application developers. Travel module users are also provided individual, in-depth training by the application developers.
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).	CFSAN retains and disposes of all data in accordance with General Records Schedule (GRS) 2.1 Employee Acquisition Records

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 role-based access restriction, 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 uses of firewalls, access controls, encryption of files, certificates or logs, and regular testing of information technology systems. 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:**	6/12/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/13/2025
SOP Review Comments:		**# of Days - SOP Review:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/13/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/13/2025 All comments have been addressed. This PIA is ready for SAOP review and approval. 6/5/2025 Please see comments and update accordingly: PTA-5: Per PIA-22, please include the following PII elements in your response: Passport Numbers, Education Records, and Personal email address and phone number. PIA-44: GRS 1 item 7c(2) was rescinded in 2017 and is no longer valid. It was replaced by nine new General Records Schedules (GRS). Please review these updated GRS and select the one that best aligns with the documents or records maintained/stored in the system. GRS 2.1 Employee Acquisition Records GRS 2.2 Employee Management Records GRS 2.3 Employee Relations Records GRS 2.4 Employee Compensation and Benefits Recor GRS 5.1 Common Office Records GRS 5.2 Transitory and Intermediary Records GRS 5.6 Security Records GRS 5.8 Administrative Help Desk Records GRS 6.5 Public Customer Service Records	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	11

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/24/2025 3:35 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 05	BLAND, CRYSTAL	6/5/2025	Per PIA-22, please include the following PII elements in your response: Passport Numbers, Education Records, and Personal email address and phone number.	
PIA 44	BLAND, CRYSTAL	6/5/2025	GRS 1 item 7c(2) was rescinded in 2017 and is no longer valid. It was replaced by nine new General Records Schedules (GRS). Please review these updated GRS and select the one that best aligns with the documents or records maintained/stored in the system. GRS 2.1 Employee Acquisition Records — DAA-GRS-2014-0002 GRS 2.2 Employee Management Records — DAA-GRS-2017-0007 GRS 2.3 Employee Relations Records — DAA-GRS-2015-0007 GRS 2.4 Employee Compensation and Benefits Records — DAA-GRS-2016-0015 GRS 5.1 Common Office Records — DAA-GRS-2016-0016 GRS 5.2 Transitory and Intermediary Records — DAA-GRS-2017-0003 GRS 5.6 Security Records — DAA-GRS-2017-0006 GRS 5.8 Administrative Help Desk Records — DAA-GRS-2017-0001 GRS 6.5 Public Customer Service Records — DAA-GRS-2017-0002	