PTA / PIA: FDA - OC OFBA SalesForce - QTR2 - 2025 - FDA4919319

Created Date: 5/5/2025 12:24 PM Last Updated: 5/20/2025 4:35 PM

General Information

PTA / PIA Name:	FDA - OC OFBA SalesForce - QTR2 - 2025 - FDA4919319	**PTA / PIA ID:**	3140804
Component Name:	FDA - OC OFBA SalesForce	**ATO Boundary Name:**	OC Office of Finance, Budget and Acquisitions Salesforce Organization
Overall Status:	Complete	**# of Days - Open:**	15
Submitter:		**Submit Date:**	5/5/2025
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?	Yes
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.	4/5/2023
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	POC Name: Cristian Bellagamba
PTA 01A:	POC Title and Organization	POC Title: Financial Systems Analyst POC Organization: OO/OC/OFBAP
PTA 01B:	POC Email Address	cristian.bellagamba@fda.hhs.gov
PTA 01C:	POC Phone Number	2404022834
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(s) of the Office of Finance, Budget, and Acquisitions (OFBA) Salesforce Org is to provide a platform to develop applications to improve or automate OFBA processes. Specifically, OFBA has developed various applications to increase efficiency, effectiveness, and improve overall transparency and communication throughout the Food and Drug Administration (FDA). OFBA has made a decision to create their own Org. This Org is OFBA's unique identifier and is its version of Salesforce's Force.com platform containing its data within the Government Cloud. OFBA Salesforce Org is configured with SSO and Network only access configurations to restrict the Internet Protocol (IP) ranges. The relationship of the OFBA Salesforce Org to other FDA systems/components/information collections is dependent on the sub applications. Each application is developed to fulfil a specific process/need and has specific requirements. The key functional elements of the system include the following applications: Purchase Card (PCard)- Purchase Card Applicant submission portal and application management solution that streamlines the PCard application approval process through automation of manual tasks to improve compliance and provided enhanced transparency through the application process. Travel Card Application - Travel Card Applicant submission portal and application management to automate the submission and tiered approval process for FDA employees seeking to obtain an FDA Travel Card while providing insights on application tracking to address process delays. Conference Leadership Evaluation and Reporting (CLEAR) - The CLEAR tool allows for the centralization and management of Conference related approvals, costs, and expenses to improve legislative compliance on reporting of Conference related activities. The CLEAR Tool includes a Robotic Process Automation (RPA) integration to migrate Conference Cost related data from ConcurGov to CLEAR. Travel Compliance Application - The Travel Compliance tool allows for the centralization and management of travel transaction audits findings to improve FDA's compliance with travel regulations. System "users" consist of consists of FDA employees and Direct Contractors. Access to components and functionality is restricted via assigned roles and profiles. The application is web based. Users access the website using FDA Single Sign-On (SSO) and Person Identity Verification (PIV) cards.

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: Employee name, employee email (business/personal), employee address (business/personal), employee travel transactions The types of data that are maintained in and/or shared from the system is/are: Employee name, employee email(business/personal), employee address (business/personal), employee travel transactions. The amount of time the PII is stored in the system is: Until system retirement
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 employees is collected and/or maintained in order to accomplish programmatic requirements and travel compliance. PII from the system/component/collection is shared with HHS and FDA entities as required to accomplish the program goals as follows: The key functional elements of the system include the following applications: Purchase Card - Purchase Card Applicant submission portal and application management solution that streamlines the PCard application approval process through automation of manual tasks to improve compliance and provided enhanced transparency through the application process. Travel Card Application - Travel Card Applicant submission portal and application management to automate the submission and tiered approval process for FDA employees seeking to obtain an FDA Travel Card while providing insights on application tracking to address process delays. Conference Leadership Evaluation and Reporting (CLEAR) - The CLEAR tool allows for the centralization and management of Conference related approvals, costs, and expenses to improve legislative compliance on reporting of Conference related activities. The CLEAR Tool includes a RPA integration to migrate Conference Cost related data from ConcurGov to CLEAR. Travel Compliance Application - The Travel Compliance tool allows for the centralization and management of travel transaction audits findings to improve FDA's compliance with travel regulations.
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).	URLs require access through FDA Secure gateway and/or SSO. https://ofba.lightning.force.com/ https://ofba.my.salesforce.com https://ofba.my.site.com/PCard/s/
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 provide user access to the following applications: Purchase Card (PCard)- Purchase Card Applicant submission portal and application management solution. Travel Card Application - Travel Card Applicant submission portal and application management. Conference Leadership Evaluation and Reporting (CLEAR) - The CLEAR tool allows for the centralization and management of Conference related approvals, costs, and expenses to improve legislative compliance on reporting of Conference related activities. Travel Compliance Application - The Travel Compliance tool allows for the centralization and management of travel transaction audits. System "users" consist of consists of FDA employees and Direct Contractors. The application is web based. Users access the website using FDA Single Sign-On (SSO) and Person Identity Verification (PIV) cards. Users access the website via https://ofba.my.salesforce.com. The following categories of individuals have access to the website user, administrators, developers.
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 Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	Individuals may enter personal phone number, address, email and other information dependent on work location. However, personal information is not required. Additionally, employee travel transaction details may be collected.
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.	10,000 – 49,999
PIA 25:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of completing programmatic application, compliance and reporting objectives, and relating records to the employee.
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: 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. Executive Order 11348 and 44 U.S.C. section 3102. And generally, 5 U.S.C. sections 4101 and 4118, and 44 U.S.C. sections 2901 and 2904. Executive Order 12934, Federal Procurement Reform. Federal Travel Regulation (FTR), 41 CFR
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	The PII data elements that are used to retrieve records in the system/system component/information collection are name and email address of current and former FDA employees.

PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	The System of Records Notice(s) (SORN(s)) used to cover the system is: SORN 1: OPM/GOVT-1, General Personnel Records url: www.federalregister.gov/documents/2023/08/17/2023-17651/privacy-act-of-1974-system-of-records SORN 2: GSA/GOVT–3,Travel Charge Card Program url: www.federalregister.gov/documents/2013/04/03/2013-07669/privacy-act-of-1974-notice-of-revised-system-of-records SORN 3: GSA/GOVT–6, GSA SmartPay Purchase Charge Card Program url: www.federalregister.gov/documents/2008/04/25/E8-8883/privacy-act-of-1974-notice-of-updated-systems-of-records
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 Other HHS 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.	This system/component does not collect information using an information collection request as defined by the Paperwork Reduction Act.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	PII from the system/component/collection is shared with HHS and FDA entities as required to accomplish the program goals through application approval processes, tracking, and compliance reporting and regulatory compliance.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	Contractor access to information is addressed in the contract between FDA and the Contractor as well as signed Non-Disclosure Agreements between the FDA and all contractor personnel with access to OFBA SalesForce data. Direct Contractors are required to adhere to the same laws, regulations, policies, and procedures as permanent employees. Both Direct Contractors and permanent employees are subject to civil and criminal penalties, including the criminal penalty provisions of the Privacy Act, applicable in the event of violations.

PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	If records in the system are shared outside of HHS, the FDA will maintain a listing of disclosures for which an accounting is required pursuant to the Privacy Act, 5 U.S.C. 552a(c). Note that under FDA regulations and Federal court decisions, contractor personnel operating this system on behalf of the FDA are considered agency employees and therefore the accounting requirement does not apply to disclosures to employees of the contractor operating this system.
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 are no opt out procedures specific to the system. Users provide their contact information as a requirement to complete application and travel. Users can elect to not provide the information as part of the application process, which may impact the FDA-related work that they are required to do per their job duties.
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.	FDA does not anticipate any major change that would affect individuals' privacy. In the event of a major change, the agency will notify individuals whose PII is in the system by the most efficient and effective means available and appropriate to the specific change(s). This may include a formal process involving written and/or electronic notice such as additional or revised privacy notices and/or Privacy Act Statements provided within the system and the online course materials, or informal processes such as e-mail notice to the individuals.
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.	FDA employees may contact a system administrator or the Employee Resource and Information Center (ERIC). Employees with such concerns can additionally work with their supervisors, the Privacy Office, a 24-hour technical assistance line, and FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). Contact information for these offices and resources is available across FDA's internet and intranet pages. All personnel are required to report suspected instances of PII compromise or misuse to FDA's 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 PII is provided voluntarily by the individual. 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. Relevancy is supported by design of system and related processes to solicit or collect only the PII necessary for the system's purpose and supporting functionality. 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 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.
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 Third-Party Contractor (Contractors other than HHS 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 - submitters 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 direct Contractors and third-party contractors are developers and system administrators.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The administrative procedures in place to determine which system users may access PII are determined by the user roles upon account provisioning.
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.	The following technical methods are in place to allow those with access to PII to only access the minimum amount of information necessary to perform the job: application of user roles. Only the minimal amount of PII data is collected by the system. The system also employs Role-Based Access Control (RBAC) which ensures users have the minimum level of access required to complete day-to-day job duties.
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.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users however users are provided with user guides and manuals, and privacy guidance is 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).	Records are managed in accordance with National Archives and Records Administration (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:**	5/5/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/5/2025
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:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/8/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 5/8/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	3

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/20/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	12

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/20/2025 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	5/6/2025	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 4/5/2023. 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.	5-6-2025 EMAIL_PIA in Queue (OC OFBA SalesForce).pdf OC OFBA SalesForce_SOP Approved_5.5.2025.pdf