Privacy Impact Assessment (PIA): FDA - ALP - QTR3 - 2024 - FDA3562152

Created Date: 8/20/2024 12:05 PM Last Updated: 8/28/2024 2:01 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	FDA - ALP - QTR3 - 2024 - FDA3562152	**PIA ID:**	2134183
Name of Component:	FDA - OC Acquisition Lifecycle Platform	**Name of ATO Boundary:**	OC Digital Solution Partners Appian
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	14
Submission Status:	Submitted	**Submit Date:**	8/19/2024
Next Assessment Date:	N/A	**Expiration Date:**	8/28/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA3562152
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	9/8/2023
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	The Food and Drug Administration (FDA) Office of the Commissioner (OC), Office of Acquisition and Grant Services (OAGS) Acquisition Life Cycle Platform (ALP) is a work management and tracking system. OC OAGS ALP is one component of the OC Digital Solution Partners (DSP) Appian system boundary (other components are separately assessed). FDA programs use OC OAGS ALP to submit acquisition materials for internal review and processing and managing acquisition services, such as interagency agreements (IAA), requests for new contracts, re-competition of current FDA contracts, and modifications to current contracts. System users consist of FDA permanent employees and Direct Contractors. DSP Administrators are contractors who require access to run reports on acquisition business metrics; manage user access; and manage data elements in the system. Users submit requests to OAGS via the ALP system. OAGS receives and assigns these requests to its staff, and staff and the requiring offices (offices seeking to acquire/contract for products and services) collaborate through the system to get the request awarded as a contract or IAA. Users of the system can view and generate reports, as well as query the system database using available system fields. Personally identifiable information (PII) is collected from FDA permanent employees, Direct Contractors, and vendors. The names and email addresses of authorized FDA users of the system are used for identification, assignment, and communication purposes only. Records in the system are not about individuals. System records consists only of acquisition lifecycle data managed by FDA.

PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The OC OAGS ALP system collects and maintains the following personally identifiable information (PII) about FDA permanent employees and Direct Contractors: a) name; b) work email address; c) work mailing address; and d) work phone number. OC OAGS ALP also collects and maintains the following vendor information: a) name; b) email address; c) mailing address; d) phone number; e) user comments; f) federal training certificates and federal acquisition certification-contracting officer representative (FAC- COR) documentation; and f) legal documentation (contracts). The following non-PII is collected and maintained in the OC OAGS ALP system: a) acquisition planning information (to include titles, descriptions of acquisitions, estimated dollar amounts, and other descriptive elements typically associated with planning); b) numbers identifying contracts, IAAs, and requisitions (funding documents); c) acquisition pre-award process completion dates (milestone dates); d) processing times; e) quality issues; f) statement of work (SOW); g) independent government cost estimates; h) acquisition plans; and i) supplemental administrative documents. Non-PII may become PII if combined with other PII data elements in system. FDA permanent employee and Direct Contractor PII is used to identify the assigned FDA point of contact (POC) for each service request submitted to OAGS and their role in the acquisition/IAA in the request. Associated system records are not about the individual POCs submitting requests or processing requests. Records in the system are about FDA acquisition lifecycle and consists of business-related content only. System access is controlled via Single-Sign-On (SSO) and no usernames/passwords are required to access the system. PII is maintained in the system until removed by the system administrator. Data within federal records are maintained according to applicable records schedules.
PTA - 5A:	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. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	The OC OAGS ALP system collects information for several related purposes. Information is collected to facilitate the immediate assignment and review of request submissions to an appropriate staff person in OAGS for processing; to accurately identify the relevant POC in the requiring FDA office for the purposes of requesting revisions or clarifications on documentation, securing approval prior to issuing a solicitation or IAA, as well as planning the evaluation process; to facilitate data analysis on areas of future improvement to OAGS, such as future educational needs or targeted customer support for specific types of acquisitions; to report on OAGS' service delivery goals and metrics, such as Key Performance Indicators (KPIs) for Service Level Agreements (SLAs); and to streamline and better organize the acquisition pre-award process by integrating request documentation with the request itself. An essential part of the requisition approval process is the identification and matching of service requests with the POC assigned to the request. PII is shared internally with authorized users for identification and matching purposes only. (e.g., users have the ability to see what HHS emails are assigned to a request and what roles they are associated to for that request. System records collected and maintained in the OC OAGS ALP system are not about the individuals assigned/managing an acquisition request. Records in the system are about the acquisitions themselves and consists only of acquisition lifecycle business content. OC OAGS ALP is not a Privacy Act system of records.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	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 FDA employees with an online portal to submit and manage acquisition services, such as interagency agreements (IAA), requests for new contracts, re-competition of current FDA contracts, and contract modifications. The website is only accessible via the FDA Network for HHS internal employees and access is granted through FDA email log in/SSO only.
PTA - 10:	Does the website have a posted privacy notice?	No
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	

PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Email Address Phone numbers Mailing Address Other - Free text Field - Legal documents, certificates, name
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of identifying the assigned POC for each service request submitted to OAGS and their role in the particular acquisition/IAA in the request.

PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no secondary uses.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	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 Departmental Regulations and the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	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.	
PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	There is currently no associated OMB form for use with the ALP system as OC OAGS ALP supports an internal FDA procurement process and does not collect any information from members of the public.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	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.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	

PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	While PII is submitted on a voluntary basis, individuals must provide their PII to use the ALP system. Individuals who have been added to a request may request to be removed from the request. Each request must have at least one name associated with it (the request submitter, who creates the request). Others are optional. The request submitter may have themselves removed and replaced by another individual via a request to the Employee Resource and Information Center (ERIC).
PIA - 14:	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). Alternatively, describe why they cannot be notified or have their consent obtained.	At this time there are no foreseeable changes planned or anticipated that will impact PII collected and stored in the system. However, in the event such a change is made, all registered system users will be appropriately notified via email using the ALP program inbox.
PIA - 15:	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 a number of avenues available for assistance. FDA personnel may submit concerns to their supervisor, the FDA Privacy Office, the Employee Resource and Information Center (ERIC), and FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) via methods listed on fda.gov and/or the FDA intranet. In the event of a suspected incident or data breach, FDA personnel who become aware of such an event must report that without delay to the FDA's CIOCC.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. 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 User Access Review at 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 (role-based access). Integrity and availability of PII 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 and 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 - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors

PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Access is required for processing government requirements into acquisitions and interagency agreements. Administrators: Access is required to run report on acquisition business metrics; managing user access; and managing data elements in system. Contractors: DSP Administrators are contractors whose access is required to run report on acquisition business metrics; managing user access; and managing data elements in system.
PIA - 19:	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 is the same for all users. FDA users (permanent and Direct Contractors) and third-party system administrator with valid network accounts who require access to the system must obtain supervisory approval and signature before access is granted. The relevant supervisor will indicate on the user account creation form the minimum access that is required for the user to complete their job. Scope of access is restricted based on role-based criteria. The agency reviews the system user access list on a quarterly basis to verify, update, and/or adjust users' access roles and permissions. Access is determined by job function (role-based). Information contained in the system is only shared on a need-to-know basis.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job. Multi-factor authentication and identity authentication support role-based restrictions.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system 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. The FDA Office of Digital Transformation (ODT) verifies that individuals successfully complete the training. All FDA employees are required to complete standard information Security Awareness Training and Privacy Awareness Training annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users of the system do not receive system specific training, however all personnel receive general privacy and security awareness training. Additionally, all system users are provided with user guides and manuals.

PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	System records including those that contain PII are retained in accordance with the following General Records Schedules: GRS 1.1 Item 010: Financial Transaction Records to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting - Official Record Held in the Office of Record-Temporary-Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. GRS 1.1 Item 011: Financial Transaction Records to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting – All Other Copies-Temporary-Destroy when business use ceases. GRS 1.3 Item 020: Budget Execution Records-Temporary-Destroy 6 years after close of fiscal year but longer retention is authorized if required for business use.
PIA - 24:	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 continuous network monitoring, secure authentication, encryption and use of firewalls. As a Software as a service (SaaS) system on a FEDRAMP cloud solution, all physical controls are inherited. Physical controls include lock and key security of space and equipment and guarded facilities.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	8/20/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP 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.	**SOP Review Date:**	8/20/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/21/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte This PIA is ready for SAOP review an approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	8/28/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	VILLAFUERTE, NESTOR	8/21/2024	Reviewer notes that the system does not have an ATO, however, the planned ATO date stated in the PIA has already passed.	
PIA - 24	VILLAFUERTE, NESTOR	8/21/2024	Please write out acronym FEDRAMP	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	8/28/2024 2:01 PM	**History Log:**	View History Log