Privacy Impact Assessment (PIA): FDA - ZPA - QTR4 - 2024 - FDA4564005

Created Date: 11/5/2024 11:23 AM Last Updated: 11/14/2024 2:51 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 - ZPA - QTR4 - 2024 - FDA4564005	**PIA ID:**	2404846
Name of Component:	FDA - OC Zscaler Private Access	**Name of ATO Boundary:**	OC Zscaler Security Suite
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	10
Submission Status:	Submitted	**Submit Date:**	11/4/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4564005
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?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	4/13/2023
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 Interagency Uses
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Since the last approved PTA/PIA, Zscaler has completed the proof of concept phase and is now fully operational.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Contractor

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.	In support of the Food and Drug Administration's (FDA's) continuing efforts to modernize and enhance FDA's Information Technology (IT) infrastructure, the Office of the Commissioner (OC) Zscaler Security Suite provides the FDA with a Zero trust-centric solution for network services that serves as a replacement for traditional virtual private network (VPN) connectivity. This on-demand, secure access service edge (SASE) technology solution provides a fast, smooth, secure, and enjoyable customer experience when accessing cloud, remote, and on-premises FDA services. OC Zscaler Private Access (ZPA) is one of two components falling under the Zscaler Security Suite system boundary (the other, OC Zscaler Internet Access or ZIA, is the subject of a sperate assessment). OC ZPA is a cloud-based, elastically scalable infrastructure connection solution that delivers connectivity to FDA's private internal applications and assets hosted in the cloud and on-premises. Leveraging FDA single sign-on (SSO) and multi-factor authentication, OC ZPA connects and restricts user access to only the applications and destinations a user is authorized to access. OC ZPA renders all FDA hosted applications and assets both invisible and unrouteable to all but authorized users authenticated to the FDA network from approved devices. Users of the system are FDA Zscaler Administrators (Admins). Non-FDA Admins and customers do not have access to the system.
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.	OC ZPA collects the following personally identifiable information (PII) from OC ZPA Admins (FDA employees and Direct Contractors): username. OC ZPA also collects the following information: dynamic Internet Protocol (IP) addresses, Unform Resource Locators (URLs), and user group and department information from a corporate directory. However, collection of this information is not used to retrieve records about users of the system. Usernames are maintained on a temporary basis.
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.	Usernames are collected from OC ZPA system Admins (FDA permanent employees and Direct Contractors). The collection and storage of this information is necessary for authentication and to ensure network access. OC ZPA also collects and stores a limited amount of machine related data (e.g., IP addresses, URLs, user groups and departments from corporate directory) that is not used for user identification purposes.
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 OC Zscaler Admins access to the system to complete testing, troubleshooting and maintenance. FDA Zscaler Admins access the website via SSO authentication. Only ZPA Admins can access the Zscaler Portal using an internal URL. Non-Admin FDA personnel and customers do not have access to the website.
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 - 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?	Yes
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	Third-party
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.	The purpose of Zscaler Client Connector for mobile devices such as iOS and Android is to provide a lightweight agent for user endpoints, enabling hybrid work through secure, fast, reliable access to any app over any network.
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
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?	No
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?	No
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.	User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ 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 multi-factor authentication (e.g., PIV credentials).
PIA - 5:	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 - 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 is 5 U.S.C 301.
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.	Directly from an individual about whom the information pertains Other Government Sources Other
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.	An OMB information collection approval number is not required as there are no forms in use and information is not collected from 10 or more members of the general 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.	Individuals may opt-out of the collection or use of their PII by not using OC ZPA. However, the submission of PII is a practical necessity to access FDA's network and failure to do so would prevent the individual from carrying out their job duties.
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.	Major changes to the system are not anticipated at this time. If the FDA changes its practices with regard to the collection or handling of PII related to OC ZPA, 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 e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.
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 to resolve the situation. Employees 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). FDA personnel are required to immediately report suspected and confirmed breaches of PII 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 to this system and any FDA source systems. 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 necessary to be granted access to the system. PII relevancy is supported through the design of the system to require and collect only those 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). 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. Integrity and availability are protected by privacy and security controls selected and implemented in the course of 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.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Administrators: To operate and administer the system and troubleshoot; access also required for usage tracking purposes.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrative access to the Zscaler consoles is restricted to personnel supporting Zscaler operations in the FDA. Only Zscaler Admins would have access to these resources.
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.	The scope of access is restricted based on role-based criteria and minimum access required to perform job duties. System settings and access credentials are applied to enforce access 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 complete annual mandatory 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 and documents that training has been successfully completed.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available via FDA's Privacy Office.
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).	The specific NARA records schedule is GRS 3.2 Item 031-System Access Records. Systems requiring special accountability for access, and the retention schedule and retention period(s) is: TEMPORARY. Destroy 6 years after password is altered or user account is terminated, 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 the concept of least privilege when providing access. Technical Safeguards include application controls, database encrypted at rest, 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 privacy and security 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 Processing (FIPS) 199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	11/5/2024
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:**	11/5/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	11/7/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/7/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Q-3 "Does the system have or is it covered by a Security Authorization to Operate (ATO)? The FDA instance of Archer is reflecting "No" as the answer when the correct answer is "Yes." The FDA Archer Team is aware of this occurrence and is working on a solution.	**SAOP Review Date:**	11/14/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(11-6-2024) EMAIL_PIA in Queue (OC Zscaler Private Access).pdf	282934	.pdf	11/6/2024 8:58 AM	0
OC Zscaler Private Access_SOP Approved.rtf	770872	.rtf	11/6/2024 8:58 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	11/6/2024	Per FDA's email: The PIA is currently 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)? The FDA instance of Archer is reflecting “No” as the answer when the correct answer is “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	

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:	11/14/2024 2:51 PM	**History Log:**	View History Log