

## 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

<b>PIA Name:</b>	FDA - ZIA - QTR4 - 2024 - FDA4318403	<b>PIA ID:</b>	2300992
<b>Name of Component:</b>	FDA - OC Zscaler Internet Access	<b>Name of ATO Boundary:</b>	OC Zscaler Security Suite
<b>Overall Status:</b>		<b>PIA Queue:</b>	
<b>Submitter:</b>		<b># Days Open:</b>	15
<b>Submission Status:</b>	Submitted	<b>Submit Date:</b>	10/8/2024
<b>Next Assessment Date:</b>	N/A	<b>Expiration Date:</b>	1/1/2100
<b>Office:</b>		<b>OPDIV:</b>	FDA
<b>Security Categorization:</b>		<b>OpDiv PIA ID:</b>	FDA4318403
<b>Legacy PIA ID:</b>		<b>Make PIA available to Public?:</b>	No
<b>1:</b>	Identify the Enterprise Performance Lifecycle Phase of the system.		Operations and Maintenance
<b>2:</b>	Is this a FISMA-Reportable system?		No
<b>3:</b>	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		No
<b>4:</b>	ATO Date or Planned ATO Date.		4/13/2023
<b>5:</b>	Is the system or electronic information collection, agency or contractor operated?		Agency

## PTA

### PTA

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

<b>PTA - 4:</b>	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 will serve 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. One component of the Zscaler Security Suite boundary is Zscaler Internet Access (ZIA), a cloud-based solution that enables fast and secure access to the internet. Access to OC ZIA is limited to FDA Zscaler system administrators (Admins) who access the administrative portal via single sign-on (SSO) authentication. FDA general users (permanent employees and Direct Contractors) and customers do not have access to this website.
<b>PTA - 5:</b>	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.	<p>OC ZIA collects the following personally identifiable information (PII): username. Usernames are only collected from Zscaler Admins who are FDA permanent employees and Direct Contractors. Usernames are required to access OC ZIA to perform job duties. OC ZIA does not collect, maintain, transmit, share or process any other PII.</p> <p>OC Zia also collects the following information: dynamic internet protocol (IP) addresses, URLs, and user group and department information from a corporate directory. However, collection of this information is not used to directly identify users of the system. The collected dynamic IP address itself is not linkable to an individual.</p> <p>Usernames are maintained on a temporary basis.</p>
<b>PTA - 5A:</b>	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
<b>PTA - 5B:</b>	Please identify the type of user credentials used to access the system.	
<b>PTA - 6:</b>	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 FDA permanent employees and Direct Contractors. The collection and storage of this information is necessary for authentication and to ensure network access. OC ZIA 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.
<b>PTA - 7:</b>	Does the system collect, maintain, use or share PII?	Yes
<b>PTA - 7A:</b>	Does this include Sensitive PII as defined by HHS?	No
<b>PTA - 8:</b>	Does the system include a website or online application?	Yes

<b>PTA - 8A:</b>	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
<b>PTA - 9:</b>	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 OC ZIA website is to provide FDA Zscaler Administrators (Admins) access to the system to complete testing, troubleshooting and maintenance. Only FDA Zscaler Admins can access the website and do so via the SSO authentication process. Non-Admin FDA personnel do not have access to the website.
<b>PTA - 10:</b>	Does the website have a posted privacy notice?	Yes
<b>PTA - 11:</b>	Does the website contain links to non-federal government websites external to HHS?	No
<b>PTA - 11A:</b>	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
<b>PTA - 12:</b>	Does the website use web measurement and customization technology?	No
<b>PTA - 12A:</b>	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
<b>PTA - 13:</b>	Does the website have any information or pages directed at children under the age of thirteen?	No
<b>PTA - 13A:</b>	Does the website collect PII from children under the age thirteen?	
<b>PTA - 13B:</b>	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?	
<b>PTA - 14:</b>	Does the system have a mobile application?	Yes
<b>PTA - 14A:</b>	Is the mobile application HHS developed and managed or a third-party application?	Third-party
<b>PTA - 15:</b>	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 application over any network. Users include IOS and android device users and these users access the mobile application by Zscaler Agent.
<b>PTA - 16:</b>	Does the mobile application/ have a privacy notice?	Yes
<b>PTA - 17:</b>	Does the mobile application contain links to non-federal government websites external to HHS?	No
<b>PTA - 17A:</b>	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
<b>PTA - 18:</b>	Does the mobile application use measurement and customization technology?	No
<b>PTA - 18A:</b>	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
<b>PTA - 19:</b>	Does the mobile application have any information or pages directed at children under the age of thirteen?	No
<b>PTA - 19A:</b>	Does the mobile application collect PII from children under the age thirteen?	
<b>PTA - 19B:</b>	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?	
<b>PTA - 20:</b>	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? Yes

**PIA**

**PIA**

<b>PIA - 1:</b>	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	User Credentials
<b>PIA - 2:</b>	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
<b>PIA - 3:</b>	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
<b>PIA - 4:</b>	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of multi-factor authentication.
<b>PIA - 5:</b>	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.
<b>PIA - 6:</b>	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
<b>PIA - 6A:</b>	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
<b>PIA - 7:</b>	Identify legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. 301 provides the legal authority governing information use and disclosures specific to the system and program.
<b>PIA - 8:</b>	Are records in the system retrieved by one or more PII data elements?	No
<b>PIA - 8A:</b>	Please specify which PII data elements are used to retrieve records.	
<b>PIA - 8B:</b>	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.	
<b>PIA - 9:</b>	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains  In-person  Government Sources  Other
<b>PIA - 10:</b>	Is there an Office of Management and Budget (OMB) information collection approval number?	No
<b>PIA - 10A:</b>	Provide the information collection approval number.	
<b>PIA - 10B:</b>	Identify the OMB information collection approval number expiration date.	
<b>PIA - 10C:</b>	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.
<b>PIA - 11:</b>	Is the PII shared with other organizations outside the system's Operating Division?	No
<b>PIA - 11A:</b>	Identify with whom the PII is shared or disclosed.	
<b>PIA - 11B:</b>	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
<b>PIA - 11C:</b>	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)).	

<b>PIA - 11D:</b>	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.	
<b>PIA - 12:</b>	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
<b>PIA - 12A:</b>	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
<b>PIA - 13:</b>	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 ZIA. 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.
<b>PIA - 14:</b>	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 ZIA, 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.
<b>PIA - 15:</b>	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 only).  FDA personnel are required to immediately report suspected and confirmed breaches of PII to the FDA's CIOCC.

<b>PIA - 16:</b>	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.	<p>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.</p> <p>Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access).</p> <p>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.</p> <p>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.</p>
<b>PIA - 17:</b>	Identify who will have access to the PII in the system.	Administrators
<b>PIA - 17A:</b>	Select the type of contractor.	Contractors
<b>PIA - 17A:</b>	Select the type of contractor.	HHS/OpDiv Direct Contractors
<b>PIA - 17B:</b>	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
<b>PIA - 18:</b>	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	<p>Users: To operate and administer the system and troubleshoot; access also required for usage tracking purposes.</p> <p>Administrators: To operate and administer the system and troubleshoot; access also required for usage tracking purposes.</p>
<b>PIA - 19:</b>	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 have access to these resources.
<b>PIA - 20:</b>	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. System settings and access credentials are applied to enforce access restrictions.

<p><b>PIA - 21:</b></p>	<p>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.</p>	<p>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 verifies that training has been successfully completed.</p>
<p><b>PIA - 22:</b></p>	<p>Describe the training system users receive (above and beyond general security and privacy awareness training).</p>	<p>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.</p>
<p><b>PIA - 23:</b></p>	<p>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).</p>	<p>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.</p>
<p><b>PIA - 24:</b></p>	<p>Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.</p>	<p>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.</p> <p>Technical Safeguards include application controls, database encrypted at rest, use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools.</p> <p>Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls.</p> <p>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.</p>

## Review & Comments

### Privacy Analyst Review

<b>OpDiv Privacy Analyst Review Status:</b>	Approved	<b>Privacy Analyst Review Date:</b>	10/9/2024
<b>Privacy Analyst Comments:</b>		<b>Privacy Analyst Days Open:</b>	

### SOP Review

<b>SOP Review Status:</b>	Approved	<b>SOP Signature:</b>	
<b>SOP Comments:</b>	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.	<b>SOP Review Date:</b>	10/9/2024
		<b>SOP Days Open:</b>	1

### Agency Privacy Analyst Review

<b>Agency Privacy Analyst Review Status:</b>	Approved	<b>Agency Privacy Analyst Review Date:</b>	10/10/2024
<b>Agency Privacy Analyst Review Comments:</b>	Reviewer: Nestor Villafuerte 10/10/2024 This PIA is ready for SAOP review and approval.	<b>Agency Privacy Analyst Days Open:</b>	1

### SAOP Review

<b>SAOP Review Status:</b>	Approved	<b>SAOP Signature:</b>	Archer Signature_Bridget Guenther.docx
<b>SAOP Comments:</b>	10/9/2024 This 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."	<b>SAOP Review Date:</b>	10/23/2024
		<b>SAOP Days Open:</b>	13

### Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
OC Zscaler Internet Access_SOP Approved.pdf	157985	.pdf	10/9/2024 8:43 AM	0

## Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	10/10/2024	<p>10/9/2024 This PIA is currently experiencing an Archer error with Question #3 of the general information.</p> <p>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."</p>	
PIA - 23	VILLAFUERTE, NESTOR	10/10/2024	Please define "GRS" and "NARA" in the first instance.	

## Admin Section

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

## Miscellaneous Fields

Last Updated:	10/23/2024 1:29 PM	History Log:	<a href="#">View History Log</a>
---------------	--------------------	--------------	----------------------------------