S. No	RFP Clause	Bid Reference	Query	Revised Clause as per Query (Requested by Vendor)	IGL Response
1	Technical Specifications, Clause No. 1 ; Page Number 60	The solution must have the capability to check device health and security posture (OS version, patch levels, AV presence and updated, encryption status, etc.) before permitting network access	Not all OEMs support each of the Posture checks mentioned. We request to relax the clause for wider participation.	The solution must have the capability to check device health and security posture (OS version, AV presence, encryption status, Registry Key etc.) before permitting network access	Tender Condition Prevails
2	Technical Specifications, Clause No. 9; Page Number 61	The solution should have the capability of multi-factor authentication	Please allow Integrated or Third-Party Integration with MFA to widen participation as not all OEMs have the MFA capability inbuilt	The solution should have the capability of multi-factor authentication (in-built or integrated with third-party MFA)	Third party Integration should be compatible with the Zero trust solution. However, bidder has to submit the documents related to integration of similair experience. Integration will be in the scope of the bidder.
3	Technical Specifications, Clause No. 10 a; Page Number 61	The solution should provide multi-factor authentication before granting access to applications.	Please allow Integrated or Third-Party Integration with MFA to widen participation as not all OEMs have the MFA capability inbuilt	The solution should provide multi-factor authentication (inbuilt or integrated with third-party MFA) before granting access to applications.	Please refer IGL response against Sr.No.2
4	Technical Specifications, Clause No. 9; Page Number 61	The Solution shall have capability, which allows solution admin to add a device on a portal, where the device goes through a registration process for network access. It should also allow admin to mark device as locked for any lost device that they have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device	This clause is very specific to a VPN OEM and not for Zero Trust Access Providers. Please delete this clause	Request to delete the clause	This clause is related to Internal network users and not for VPN users. Hence, tender conditions prevails.
5	General functionalities and specifications, Clause No. 29Page Number 60	The solution should provide a centralized interface to manage zero trust access from users who are connecting remotely from the internet as well as from Local Area Network to servers/applications deployed on-premise, in hosted data centers and in the cloud.	The clause asks for Local Area Network Analysis and control as well. Is the scope limited to Internal Apps or IGL also wants to introduce Internet Security in this RFP.	Please elaborate if Internet Security is also needed on this RFP	This is related to remotely connected users through internet and private network users (onsite users).
6	Technical Specifications, Clause No. 12 e; Page Number 61	Ability to protect on-premises as well as cloud based applications such as IaaS, PaaS and SaaS etc.	SaaS Applications are a part of Internet Applications. Please elaborate if Internet security is needed as a mandatory component to this RFP or OEM/Bidder should only focus on Internal Apps.	Please elaborate if Internet Security is also needed on this RFP	Tender Condition Prevails
7	Scope of Work , point number 17, page number 62	The Solution shall have capability, which allows solution admin to add a device on a portal, where the device goes through a registration process for network access. It should also allow admin to mark device as locked for any lost device that they have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device	N/A	The Solution shall have capability, which allows solution admin to add a device on a portal, where the device goes through a registration process for network access. It should also allow admin to mark device as locked for any lost device that they have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device or add / remove user account from admin panel and deactivate black listed device to connect to ZTA gateway.	Any additional features are welcome without any additonal financial implication.
8	Scope of Work , point number 38, page number 60	OEM should be ISO 27001:2013 complied.	Currently AccelPro Technologies India Private Limited (OEM) is not ISO 27001:2013 certified. We request you to amend this particular requirement and extend 2 years' time line to get our organization ISO certified. We also look forward to you as being Indian Cyber Security Product company and promote Make in India initiative from Government of India.	N/A	Tender Condition Prevails

9	Section 5 Technical Specifications 1	The solution must have the capability to check device health and security posture (OS version, patch levels, AV presence and updated, encryption status, etc.) before permitting network access	The solution must have the capability to check device health and security posture (OS version, AV presence and updated, encryption status, etc.) before permitting network access	Patch Levels can be checked if IGL have patch management tool (like Big Fix) and it can be integrated with FortiNAC to get latest patch details. Also confirm if OS default Encryption method is used or any third party solution is used for encryption.	Please refer IGL response against Sr.No.1
10	Section 5 Technical Specifications 3	The solution should maintain an up-to-date/centralized inventory of authorized devices connected to IGL's network (within/outside premises) and authorized devices enabling the IGL's network.	Please calrify for Outside Premises users will be connected through VPN? Which VPN solution is in production currently.	For Outside user, connectivity will be thourgh VPN or outside user connecting IGL DC resources or cloud resources.	VPN/Secure Remote Access solution will be in the scope of the bidder
11	Section 5 Technical Specifications 5 12.c	Solution must have the capability to protect unpatched systems/applications.	Please confirm which endpoint security solution is used by IGL because this requirement can be managed using Endpoint Security solution.	N/A	IGL is using EDR solution from one of the reputed OEM. Details will be shared with qualified bidder only.
12	Section 5 Technical Specifications 5 12.e	Ability to protect on-premises as well as cloud based applications such as IaaS, PaaS and SaaS etc.	Ability to protect on-premises as well as cloud based applications such as IaaS/ PaaS/ SaaS etc.	Please clarify if required any separate Firewall and Web Application Firewall for IaaS, PaaS & SaaS services.	Tender Condition Prevails
13	Section 5 General Specifications 6	All the supplied hardware & software should be with 3 years warranty and on-site support from OEM.	All the supplied hardware & software should be with 3 years warranty and on-site support from Elite Partner.	N/A	Tender Condition Prevails
14	Section 5 General Specifications 16	The system should support cloud platforms like Azure, Google Cloud, AWS & private cloud etc.	The system should support cloud platforms like Azure, AWS & private cloud etc.	N/A	Tender Condition Prevails
15	Section 5 General Specifications 36	Solution should be able to automatically bind MAC or Unique ID's of remote machines for device authentication.	Solution should be able to bind MAC or Unique ID's of remote machines for device authentication.	MAC binding can be done manually.	Solution should be able to automatically bind MAC or Unique ID's of remote machines for device authentication. Incase of manual intervention,it should be one time activity only and the same should be done by bidder onsite resource.
16	Section 5 General Specifications 38	OEM should be ISO 27001:2013 complied .	OEM should be ISO 27001:2013 or Product Safety authorities worldwide	This point is favouring single OEM	Tender Condition Prevails
17	Technical Specifications, Point-4 ; page number 60	The solution should be designed and deployed to work with the existing network and devices and should not require re-architecting the network or replacement of existing devices.	Need to understand the current inventory. We do support multiple devices mentioned in the list below https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/compatibility_doc/b_ise_sdt_30.html Please refer table 15 & 16 **Please share the total number of users and Network Devices.**	N/A	Inventory details will be shared to the qualified bidder only
18	Technical Specifications, Point-6 ; page number 61	The solution should have the feature to integrate with SOC solution/services if requires.	Forwarding of all logging information is possible. Please allow	N/A	Tender condition prevails
19	Technical Specifications, Point-8 ; page number 61	Agent installing in Desktops/Laptops should not consume RAM more than 5%.	Requesting to remove this point.	N/A	Tender condition prevails
20	Technical Specifications, Point-9 ; page number 61	The solution should have the capability of multi-factor authentication.	For VPN and Application access we can have MFA enabled by integrating other solution, for Radius Authentication we cannot have MFA enabled.	N/A	Third party Integration should be compatible with the Zero trust solution. However, bidder has to submit the documents related to integration of similair experience. Integration will be in the scope of the bidder.

21	Technical Specifications, Point-10 ; page number 61	Multi-factor Authentication a. The solution should provide multi-factor authentication before granting access to applications. b. The solution must support soft tokens preferably code generated through mobile phones & Tabs/applications/ email etc. c. The authentication should be out-of-band before the connection is allowed to the application. d. The authentication should be performed using unique digital identities and One Time Password. e. The solution should support integration with AD/LDAP. f. The solution should support deployment in High Availability mode if required. g. Product deployment should be supported on physical, virtual as well as cloud instances. However, the required hardware or virtual infra including OS and other licenses etc, is in scope of bidder.	Methods that do not prove posession of the specific device such as VOIP, Email shall not be used for out-of-band authentication. https://pages.nist.gov/800-63-FAQ/#q-b11 https://pages.nist.gov/800-63-3/sp800-63b.html#ooba Hardware / Software and license being part of bidder point should be seperated in a different row and we need to get a buy in from bidder for the same. Ideally these components are provided by customer. Please confirm	N/A	Tender Condition Prevails
22	Technical Specifications, Point-12 ; page number 61	Application Protection a. The solution must be capable of reducing the attack surface at application layer. b. Application should be visible to authenticated and authorized users / devices only. c. Solution must have the capability to protect unpatched systems/applications. d. Support must exist to protect in-house, legacy and commercial applications. e. Ability to protect on-premises as well as cloud based applications such as IaaS, PaaS and SaaS etc.	Need to understand more on this "**c. Solution must have the capability to protect unpatched systems/applications.**" We can stop access for unpatched systems but visibility for unpatched application is not there.	N/A	Any additional features are welcome without any additonal financial implication.
23	7.1- Technical BEC-Point-a ; page number 08	(a)The bidder/OEM should have successfully executed single work order of Rs. 20.22 Lacs for Implementation of Zero Trust Access Solution and support services in India during the preceding 7 years reckoned from the date of floating of tender	Please allow to submit on-going project details as an executed single PO where in complete Material have been supplied and installation is in-process against this BEC	N/A	Tender Condition Prevails
24	General functionalities and specifications; Point no 5, Page No. 59	Licenses / Subscription should be considered based on assets/devices registered with the ZTA Solution and visible on the console at any given point of time.	Zscaler Platforms works on named-user license model and hence provides user-based licenses. It allows each user to register multiple devices with a single user license, which helps optimise the overall bill of material. Kindly modify this point as follows: Licenses / Subscription should be considered based on users/assets/devices registered with the ZTA Solution and visible on the console at any given point of time.	N/A	Any additional features are welcome without any additonal financial implication.
25	N/A	All the supplied hardware & software should be with 3 years warranty and on-site support from OEM.	Zscaler Zero Trust on-premises components are all virtual and hence there is no direct dependency from the OEM. However on-site support can be provided by the bidder where ever applicable.	N/A	All the supplied hardware & software should be with 3 years warranty. OEM to provide all necessary onsite support incase bidder is unable to address the issues/problems as per SLA.

26	General functionalities and specifications; Point no 21, Page No. 60	The solution should have the capability to provide network access based on the identity of the user and device and not IP address of the device.	This point is not applicable to Zero Trust solution as Zero Trust operates at the application layer and network is just a medium for the communication. Kindly modify this point as follows to make it applicable to zero trust solution. "The solution should have the capability to provide application access based on the identity of the user and device and not just an IP address of the device."	N/A	Tender condition prevails
27	N/A	Solution should be able to automatically bind MAC or Unique ID's of remote machines for device authentication.	This point can also be validated from the MFA vendor.	N/A	Solution should be able to automatically bind MAC or Unique ID's of remote machines for device authentication. Incase of manual intervention,it should be one time activity only and the same should be done by bidder onsite resource.
28	Technical Specifications; Point No. 15, Page Number 62	The solution should enforce security policies by blocking, isolating, and reporting noncompliant machines in a quarantine area without requiring administrator attention	As per Zero Trust principle, application access should not be grated from a non-compliant devices as that can impose security threat. Hence isolation is not applicable. Zero Trust solution can allow or block access based on device compliance/non-compliance status and could report reporting noncompliant machines for administrator attention. Since isolation is not applicable in Zero Trust world, we request you to kindly modify this point as follows: "The solution should enforce security policies by blocking and reporting noncompliant machines for administrator attention."	N/A	Tender condition prevails
29	N/A	The solution should discover any new device entering the network and permit network access based upon the policy for the device.	Zero Trust operates at the application layer and network is just a medium for the communication. Hence, Zero Trust platform does not need to discover devices or control them at the network layer because security is enforced where it is needed and that is the Application layer. Kindly modify this point as follows to make it applicable to zero trust solution. "The solution should discover any new device getting registered to the Zero trust platform and permit application access based upon the policy for the device."	N/A	Tender condition prevails
30	N/A	The Solution shall have capability, which allows solution admin to add a device on a portal, where the device goes through a registration process for network access. It should also allow admin to mark device as locked for any lost device that they have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device.	This point is not applicable to Zero Trust solution as Zero Trust operates at the application layer and network is just a medium for the communication. Also, as per zero trust principles even an admin should not have a right to add a device directly as that could bypass security measures and could impose security risk. Kindly modify this point as follows to make it applicable to zero trust solution. "The Solution shall have capability, which allows solution users to register an authorized device on a portal, where the device goes through a registration process for application access. It should also allow admin to Un-register/Quarantine a device which is as lost/stolen, which prevents others from unauthorized application access when using the un-registered device."	N/A	Tender Condition Prevails

31	N/A	1. Zero Trust Access Solution should support (Hardware/Software or Hardware & Software or Cloud based) minimum 1500 users subscription / licenses (including guest users) for end points. The licenses should be on trust based during the contract validity. Solution shall use Agent based approach for Desktops, Laptops, etc. and Agentless for other devices including guest users, Network Devices, Printers/Scanners, Wireless access points, etc., for detection of unauthorized access & security posture of endpoints	Please clarify license type Concurrent/Named	N/A	Named user based on end points
32	N/A	The solution must ensure that device identity must be unique and cannot be tampered or spoofed.	Please include more device information like Hardware id, CPU ID, Motherboard ID along with mac id and device id to avoid any tampering or spoofing.	N/A	Tender Condition Prevails (Bidder can decide the other details to be included)
33	N/A	The solution must ensure that organization data remains between organization authorized end point and application.	Please include feature like blocking copy/ paste, screenshot, screen recording activity from published application to local device with ZTNA solution. We understand from this feature that there should be no public cloud connectivity between organization authorized end point and application.	N/A	Tender Condition Prevails (Only authorized and validated users can access applications)
34	N/A	Solution should be able to automatically bind MAC or Unique ID's of remote machines for device authentication.	Please include more binding information like Hard disk ID, CPU ID, Mac ID, CPU ID etc. for better authentication.	N/A	Solution should be able to automatically bind MAC or Unique ID's of remote machines for device authentication. Incase of manual intervention,it should be one time activity only and the same should be done by bidder onsite
35	Form 3 in section 7	"FORMAT FOR CERTIFICATE FROM STATUTORY AUDITOR CHARTERED ENGINEER FOR DETAILS OF SIMILAR GOODS/ WORK/ SERVICES SUPPLIED/ DONE DURING PAST 7 YEARS"	Does this form needs to be submitted by the OEM/Bidder, having shared the similar case study reference .		The form needs to be submitted by the primary bidder/OEM
36	General functionalities and specifications; Point no 7, Page No. 59	The solution should be compatible with our existing network devices & components like (Infinity Labs-SDWAN), network switches (Cisco, HP, D-Link etc) & Wi-Fi Access Points (Aruba, D-Link etc).	we request you to change the clause to be compatbile with network devices and request to exclude other hardware such as network switches, Wi-Fi access points, and Infinity Labs' SDWAN as these work on diffferent network toploy and beat the purpose of zero trust architecture . Mobile, desktop, and laptop	N/A	Tender Condition Prevails (If the OEM device is not compatible, the bidder can add devices to make the same compatible and these devices will be in the scope of bidder. IGL will not pay any additional charges)
37	IGL Technical Requirements >> Technical Parameter >> Secured Remote Access ; Page no. 10 Clause no.11 (D)	Secured Remote Access : Minimum encryption key length must be 1024-bit and above.	We kindly ask that you may limit the minimum encryption key length at 256-1024 bits because any longer would result in access delays since encryption hinders the performance and the recommended industry minimum standards also stands as 256 bits. Please refer the below given link for the Recommendation on Key Management recommended by NIST(National Institute of Standards and Technology): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf	N/A	Tender Condition Prevails

38	Tender Document >> Implementation of Zero Trust Access Solution at IGL ; Page no. 06, Clause no.07 section 1	Bid Submission Date: 04.04.2023 till 1430 hrs IST	We request you to kindly extend the Bid submission date by 3 weeks as the bidders will require time in designing the solution and filing the asked documents in the Bid.	N/A	To be discussed
39	Clause No 7.1 Technical BEC: (a)	The bidder/OEM should have successfully executed single work order of Rs. 20.22 Lacs for Implementation of Zero Trust Access Solution and support services in India during the preceding 7 years reckoned from the date of floating of tender.	Our assumption is either the Bidder directly or OEM used by Bidder has the said qualifications. Also it is assumed that Project is either executed in India or in case of overseas client, it is executed from India. Please confirm our understanding.	N/A	Credentials of OEM shall suffice to meet technical BEC
40	SOR	Zero Trust Access Solution (Software Subscription/ licences) - 3 Years	The requirement indicates that Zero Trust Access Solution (Software Subscription/ licences) - 3 Years and total required qty is 3. please clarify is it for 3years requirement or for total 9years requirement.	N/A	Total Quantity 3 = 1 year *3 (total 3 years)
41	Clause No 7.1 Technical BEC: (a)	The bidder/OEM should have successfully executed single work order of Rs. 20.22 Lacs for Implementation of Zero Trust Access Solution and support services in India during the preceding 7 years reckoned from the date of floating of tender.	Please allow bidder to submit the order copies on the behalf of OEM and as per industry norms OEM experience is considered if the bidder doesn't have the same	N/A	Please refer to IGL response Sr. No. 39
42	Clause No 7.1 Technical BEC: (a)	The bidder/OEM should have successfully executed single work order of Rs. 20.22 Lacs for Implementation of Zero Trust Access Solution and support services in India during the preceding 7 years reckoned from the date of floating of tender.	As per your above RFP , we hereby request you to allow bidder to submit OEM's experience for the Clause 7.1(a). This will ensure the bid to be competitive	N/A	Please refer to IGL response Sr. No. 39
43	Page No. 60 ,Point No. 19	The solution must ensure that device identity must be unique and cannot be tampered or spoofed.	This will not give any scope for tampering or spoofing.	The solution must calculate device context based on following parameters and allow, block and limit access of the user based on calculated context: a. User's device's unique ID that can not be modified by user b. User's device's using hardware ID with minimum 3 parameters like MAC ID, HDD ID, CPU ID, Motherboard ID c. geolocation of the device d. Device OS type and version e. Antivirus status and update status f. Windows OS update patches	Tender Condition Prevails
44	Page No. 61 ,Point No.10.e	The solution should support integration with AD/LDAP.	This will help in complying and amanaging a single user to support multiple IDs	The solution must be able to provide applications to Microsoft active directory, LDAP and workgroup users.The solution should have facility to validate user ID against LDAP using custom query to support multiple IDs against a single user	Tender Condition Prevails

45	Page No. 62 ,Point No.14	The proposed solution must support agent-based and/or agentless deployment and provide complete posture analysis. The Solution Should support all the feature & functionalities like Profiling, Posturing, Alert, & Blocking etc.	Blocking of copy/paste,screenshot,print screen etc are very important from DLP (Data Leak Prevention) perspective.	The Solution should provide on-demand and policy-based endpoint control using agent features to restrict user from copying or downloading data from IGL application to local PC. The feature must include: - Blocking copy from browser to any other application - Blocking copy from any specified application to any other application - Blocking copy from all applications but allowing specific application - Blocking print screen for whole system - Blocking all screen recording software - Blocking any software that can take snapshot of the user PC	Tender Condition Prevails
46	Page No. 60 ,Point No.31	The solution should be possible to deploy the solution with minimal changes to the underlying infrastructure setup.	OEM should have ownership if any customization support required to provide access to any web applications.	The OEM should provide customization support in case any web appIication is not supported by default in clientless mode	The solution should be possible to deploy the solution with minimal changes to the underlying infrastructure setup. However, in case customization required at the underliying infrastructure, bidder / OEM to take ownership of the same with required software, hardware, licenses etc. IGL will provide necessary support to bidder.
47	N/A	N/A	SMS service required or not, if required please confirm number of SMS required/year	N/A	IGL has own SMS Gateway.
48	N/A	N/A	One on-site manpower required for 1 year in general shift but no qualification criteria is mentioned. Kindly share the same so that manpower cost can be considered accordingly	N/A	Graduate degree with minimum 2 year experience in IT and the resource should be OEM Certified. On-boarding of the resource will be subjected to interview.